ivanti

2023 Cyberstrategy Tool Kit for Internal Buy-In

How to Win Budget and Influence Stakeholders by Explaining Why Your Cybersecurity Strategy Matters to Non-InfoSec Outsiders

in collaboration with

CSW Cyber SecurityWorks

Foreword

Welcome, stranger!

This eBook will vindicate you and your team's cyberdefense strategy for the next year, in a way that everyone at your organization can understand, fund and follow.

By the time you get to the end, this eBook will:

① **Offer your organization's non-InfoSec staff an easy-to-follow, contextualized summary** of major threat actors and their attack patterns throughout 2022, pairing panicked headlines end users see in the media with your strategic security recommendations.

② **Demonstrate** exactly how those same proactive security measures you've wanted to implement – and for everyone to use! – would have stopped devastating attacks in their tracks.

③ **Help you empower every stakeholder and end user** to feel as though they helped prevent major breaches and attacks, just by implementing and committing to what you've been asking them to do for years.

We want to help you keep your organization safe in 2023 – but not through the same reactive, "patch the headlines" approach that floods your inbox with panicked requests every other month.

Your team is burnt out, trying to follow that approach.

Your organization is burnt out!

Instead, use this eBook toolkit as your first step to show the "why" behind your defense strategy – not just the "what" – in a way that people outside of InfoSec can understand. That way, you can lay the groundwork for the investments needed to stop cyberattacks before they happen.

Show the "why" behind your cyberdefense strategy – not just the "what."

We wish you the very best of luck, stranger. May this playbook help your team get the resources, manpower and time they need to do what they do best: keeping your organization safe throughout the next year – and beyond.

Bring statistics to life through the true stories we've curated here, of organizations just like yours attacked by different cybercriminals with unique motivations and intrusion styles.

Go beyond MITRE analysis and CVE criticality to show stakeholders how small investments in "security extras" could have helped stop devastating real-world attacks, in a language and format people outside of the InfoSec world can understand.

Prove how a few months' extra time and resources would give your team a chance to test and roll out cross-organization patches or remediations without interrupting regular business operations... and before criminals could target your systems.

Contents

The Defense Directory:

How to Arm Your Employees
and Resource Your Team

ivanti | CSW Cyber SecurityWorks

Before we get to who we'll be fighting off our networks for the next twelve months, we really need to start with how your organization should prepare their defense – and that includes the tools and tactics you want to implement before a major breach occurs.

In fact, each of these chosen solutions could defend against practically every threat actor we've selected for this Tool Kit, in one way or another.

Once everyone has a clear understanding of the possible defense mechanisms that your team could deploy – given time, leadership buy-in and resources – then we'll show exactly where and how these techniques might have stopped some of the most prevalent and nefarious cyberattacks over the last few years.

Each cyberdefense tactic will include:

✓ Time to functionality and cost.

✓ A simplified description of what the defense tool is.

✓ An explanation of how it helps defend against certain types of cyberattacks.

✓ An "Arm Your People!" cheatsheet to overcome common objections from internal stakeholders and move the conversation away from "Why do you need this?" to "How can we help pay for and implement this?"

In This Section

The Defense Directory:
How to Arm Your Employees
and Resource Your Team

ivanti | CSW Cyber SecurityWorks

Anti-Phishing

Time to Functionality:

Days	Weeks	Months

Cost of Paid Tools (Entry to Robust Solutions)

$	$$	$$$	$$$$	$$$$$

Description

"Anti-phishing" often refers to a suite of tools designed to stop hackers from tricking users into clicking bad links or downloading malicious files across multiple platforms, devices, browsers, applications and text messages.

How It Helps Defend

Humans are not perfect! If a hacker manages to trick someone into clicking a link or starting a file download, these tools help prevent any malicious activity from actually occurring.

Arm Your People! – Justifying to Stakeholders

" Don't we have a filter for spam messages? Why should we get something different?

Yes, there are free tools on some browsers and emails. However, they aren't available on all platforms, and incidents are increasing as employees increasingly use personal devices for professional purposes.

" Why is anti-phishing taking so long to implement after we bought it?

List out every OS, device type, network system, browser and other endpoint your anti-phishing solution must cover. This should be enough to illustrate why it's not instantaneous!

" Why should we pay so much for these tools when there are free versions?

The increased cost for more robust anti-phishing tools is usually due to multiple platforms and devices. Credential hacking through phishing is a common tactic of nearly threat actor, no matter their end motivation.

So, anti-phishing tools might ultimately be one of the simplest and cheapest ways to prevent expensive cybersecurity breaches!

Antivirus / Antimalware

Time to Functionality:

Days   Weeks   Months

Cost of Paid Tools (Entry to Robust Solutions)

$ $$ $$$ $$$$ $$$$$
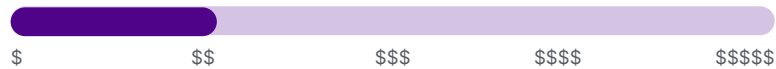
Description

This is the most basic of any cybersecurity solutions, offering broad protection and a general deterrent from basic penetration attempts.

How It Helps Defend

Essentially, antivirus and antimalware are the bare necessities any organization should implement – just to block and deter the most basic or opportunistic threats.

Arm Your People! – Justifying to Stakeholders

Why should we spend more money on this when we have built-in "free" vendor offerings?

You may be able to justify a switch to an improved antivirus or antimalware solution if the free version is slowing down computers or generally causing operational issues.

If the operational impact becomes extreme enough, then you can argue that the free software isn't worth the price. Your stakeholders will probably applaud your sourcing a new antivirus or malware tool.

Application Control

Time to Functionality:

Days   Weeks   Months

Cost of Paid Tools (Entry to Robust Solutions)

$ $$ $$$ $$$$ $$$$$
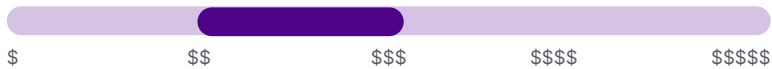
Description

Application control tools only allow certain applications within the protected environment. These controls are typically found most often in highly regulated or enterprise-level organizations.

How It Helps Defend

By only permitting applications or software from an already vetted "whitelist" of providers, application control prevents unknown payloads hiding malware and Trojan viruses from being accidentally downloaded by an employee – especially any without signed certificates.

Arm Your People! – Justifying to Stakeholders

**Why should we pay for app control?
We already have these other user controls!**

Of course, all control tools work together and layer one on another to present the best possible cyberdefense.

However, if you want to specifically budget for application control, you can tell the non-InfoSec stakeholder that application control specifically could save the company money, by monitoring application usage and eliminating unused "shelfware."

If you do this, then I can't run XYZ app that I need for my job!

This is another instance where proactive communication with all of your non-InfoSec department stakeholders is key.

Get a comprehensive list of applications currently used by all departments – and discover the ones they're paying for personally as "shadow IT" apps, if you can. Then, as part of your whitelisting process, double-check every app on that list won't present a security threat, so that business operations can continue without any significant interruption.

Then, make the process for requesting a new app to be added to protected environment as painless and fast as possible, while still guaranteeing at least one set of human eyes on each request. If you fully automate this process, then hackers could possibly take advantage and secretly grant permissions to their own activities.

Defense Directory   Threat Actors   Tactical Index

Configuration Management

Time to Functionality:

Days   Weeks   Months

Cost of Paid Tools (Entry to Robust Solutions)

$ $$ $$$ $$$$ $$$$$
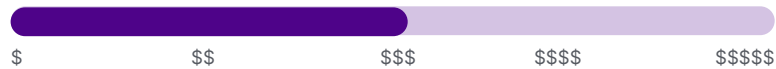
Description

Settings, ports, protocols – all of these should be accounted for in configuration management, to ensure the entire system has a secure baseline. Configuration management also includes ensuring all of the items you're paying for end up on the right devices and get used!

How It Helps Defend

Commonly open ports and configurations are publicly known by threat actors. Sticking with defaults or no-longer-supported versions create extended attack surfaces.

Configuration management can also support the overall security tech stack by ensuring that other security programs aren't forgotten or aren't set up properly on devices and environments.

Arm Your People! – Justifying to Stakeholders

Why do we need to buy configuration management?

Smaller organizations without high regulatory hurdles may find the cost-benefit analysis tipped too far on the cost side to truly see a value for configuration management tools. It can be a high-cost manual effort, too, so be sure to prove that the tool you want won't become an administrative burden on your team.

However, when done correctly, configuration management can help your organization save money by ensuring technology investments made across all departments are actually being installed.

Device Hygiene & Management

including Asset Discovery and Reconciliation

Time to Functionality:

Days — Weeks — Months

Cost of Paid Tools (Entry to Robust Solutions)

$ — $$ — $$$ — $$$$ — $$$$$

Description

For this Defense Directory, we're defining Device Hygiene and Management solutions as the tool or tool suite required to continuously find, list, monitor and react to threats in every endpoint device, hardware and software asset in your environment. For security purposes, solutions should also facilitate or integrate with any direct remediations or actions required in the event of an identified intruder.

How It Helps Defend

You can't secure what you don't know about. A cybersecurity solution set requires a robust, dynamic and automatic accounting of every endpoint in a protected network, as traditional device audits are accurate only at the single point in time at which the discovery project was finalized. Asset discovery capabilities support hygiene and management programs by spotting unaccounted for devices for protection... and possibly as a potential intruder pretending to be "just another laptop" on the network.

Arm Your People! – Justifying to Stakeholders

We have ITAM – why do we need more?

A regular ITAM tool typically tracks just the devices and assets it expects to find, from input purchase logs and active directories. Remind this stakeholder that it's what you don't see or haven't found yet that presents the biggest potential risk to impact regular business operations.

Between reconciling the active directory, procurement, endpoint management and endpoint protection systems, you might still be missing 20-30% of the assets your organization should be protecting – let alone what devices any hackers or threat actors might introduce, or any malware payloads delivered from unaccounted for BYOD programs.

Why pay for an upgrade?

As organizations increase in size, device counts rapidly expand beyond cheaper option capabilities. And single project reconciliations degrade the instant they're done.

Plus, consider that most free tools included with software suites rarely include dynamic asset discovery, which senses unknown or unaccounted for devices as they enter and exit the environment.

For security, asset discovery is a pivotal piece of the puzzle, not just a "nice to have," when it comes to managing an attack surface.
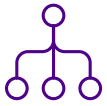
Endpoint Device & Response (EDR)

including Intrusion Detection System (IDS)
& Intrusion Prevention System (IPS)

Time to Functionality:

Days   Weeks   Months

Cost of Paid Tools (Entry to Robust Solutions)

$ $$ $$$ $$$$ $$$$$
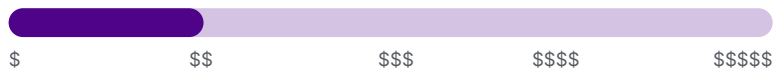
Description

EDR solutions can identify and even stop unauthorized access before it gets through. These are often paired with other initial access solutions, such as firewalls or antivirus / antimalware protections. These tools can also be on a firewall, such as detecting unauthorized IP address origins. EDR solutions can be automated to detect access patterns and traffic trends that differ from baseline, to alert to possible cyberattacks.

How It Helps Defend

You can only respond to the incidents you know about. The more alarms and traps you can set for hackers, the more attacks you'll know about – and be able to stop.

Arm Your People! – Justifying to Stakeholders

Why pay for EDR when we have a free firewall?

Explain to a non-InfoSec user that it's the difference between just having a wall, and having a wall plus gate-guards. The wall is a great deterrent, but it doesn't proactively scan for threats and try to stop them from getting through.

EDRs can be a lot of automatic security for a relatively low investment, in terms of both money and people.

Why is it taking so long to set up?

Remind your stakeholder that there's a lot behind the scenes that requires finetuning – stuff your team worries about so their teams won't even know it's there, when it's done being implemented.

Your team will also need to monitor the initial installation over a longer period of time to ensure that the EDR's output can be trusted, which may lead to tweaks that cause some rough patches even after implementation.

Defense Directory   Threat Actors   Tactical Index

Malicious Encryption Detection & Isolation

Time to Functionality:

Days   Weeks   Months

Cost of Paid Tools (Entry to Robust Solutions)

$ $$ $$$ $$$$ $$$$$
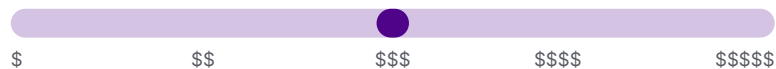
Description

When a bad actor begins to encrypt or exfiltrate files or data for ransom or theft, this type of software can automatically detect files under attack and isolate portions of the network or server to prevent further encryption.

How It Helps Defend

If all else fails, malicious encryption detection and isolation can help detect cybercriminals before they steal or lock enough data to make it hurt.

Arm Your People! – Justifying to Stakeholders

Why would we need to pay for this?

Remind your non-InfoSec stakeholder of the adage, "Expect the best, but prepare for the worst."

While your other security tools will hopefully stop cyberattacks before they reach this point, this software can act as an emergency brake when it detects encryption or exfiltration of sensitive data.

And how would the public react, if they knew you didn't take every possible, realistic opportunity to protect their information? Or your shareholders, to insulate their investment from theft of intellectual property?

We have cyberinsurance, why bother going any further?

Cyberinsurance can help you pay for the damage control and clean up, but it will still be astronomically cheaper and easier to deal with a media statement about a stopped intrusion, rather than clean up after a full-blown breach.

Your insurance rates would also skyrocket, and probably require additional – and perhaps even more expensive – safeguards to be put in place, just to be able to be insurable.

Defense Directory   Threat Actors   Tactical Index

Network Segmentation

Time to Functionality:

Days — Weeks — Months

Cost of Paid Tools (Entry to Robust Solutions)

$ $$ $$$ $$$$ $$$$$

Description

Network segmentation is the division of an organization's internet and intranet networks, so that only certain devices can access certain parts of applications or servers. It can be as simple as Internet of Things (IoT)-enabled devices on their own network segment, to as complicated as each department and server with its own environment and network.

How It Helps Defend

Network segmentation prevents hackers from being able to access any other part of the network that their original compromised credentials or access point couldn't access. If an attacker makes it into a benign part of your environment – such as an IoT-enabled toaster oven, for example – they don't have greater access to anything sensitive.

Arm Your People! – Justifying to Stakeholders

Why should we pay this much for a network segmentation tool?

Network segmentation tools can save the security team time and resources, identifying network intruders and making authorized flow between environments more intuitive.

So, remind your non-InfoSec stakeholder that with less time managing or monitoring networks, you can get to the other items they've asked of your team.

And, the more sophisticated a tool you get, the less of a hassle it'll be for their team to move from one network segment to another, when needed.

Why is it so hard to get the documents I need out of this environment now?

Try to make the process for your non-InfoSec stakeholders to submit change permission requests as simple and intuitive as possible.

Remind your team to be as patient as they can with any complaints – especially at the start! You can minimize many of these complaints by proactively including leads from all departments in the implementation process as project-consultants, telling you who needs access to which segments and their general workflows.

Defense Directory   Threat Actors   Tactical Index

Passwordless Multi-factor Authentication (MFA)

Time to Functionality:

Days   Weeks   Months

Cost of Paid Tools (Entry to Robust Solutions)

$ $$ $$$ $$$$ $$$$$
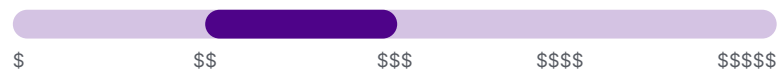
Description

Passwordless MFA are login tools that require a secondary authentication – via text / SMS, email, authenticator app requests, or even biometric data – for access to applications or granting permissions. Unlike traditional two-factor MFA, however, passwordless MFA logins do not require a password.

How It Helps Defend

As a rule, the average non-InfoSec employee will avoid creating complicated or unique passwords. By eliminating passwords, hackers can't access systems through credential stuffing, brute force passwords, or an employee leaving their password out on a sticky note.

Plus, passwordless MFA programs can help increase compliance with security programs, since it's one less thing for them to remember!

Arm Your People! – Justifying to Stakeholders

Why does passwordless MFA cost so much more than alternatives?

There's a range of passwordless MFA tools available. Generally speaking, the higher the per user cost, the higher the encryption levels and custom controls available.

Better encryption helps keep hackers from breaking the system with sheer computer power.

And, custom controls can help decrease labor costs while making it more user friendly for everyone.

The time-out sessions are so annoying! Can you stop them?

First, depending on the relationship you have with the stakeholder, you can joke around and say, "If you think they're annoying, imagine how much more frustrating it is for a hacker to constantly get kicked out! At least you can get back in."

Then – more seriously – you can show the non-InfoSec stakeholder that gaining access to the network is just the first part of a cyberattack, with some of the Defense Plays later in this eBook. The harder the organization makes it for unauthorized hackers to stay in, the easier it will be for your team to detect the invasion and kick them out for good.

Defense Directory   Threat Actors   Tactical Index

Privilege Management

Time to Functionality:

Days   Weeks   Months

Cost of Paid Tools (Entry to Robust Solutions)

$ $$ $$$ $$$$ $$$$$
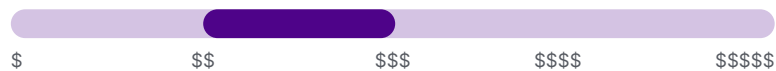
Description

Privilege management controls which types of employees need which permissions on their personal or network machines. For example, the average office worker could probably use power admin status on their personal machines, but generally do not need permissions to install PowerShell.

How It Helps Defend

Similarly to access control, if a hacker accessed the average employee's desktop computer – for which that employee was logged in as a super admin – they still wouldn't be able to deploy many hacking tools and gain greater network access, due to the limited permissions.

Arm Your People! – Justifying to Stakeholders

Why should we pay for this, too? It will take more man power to deploy and manage!

Yes, as a rule, it can take more labor to implement and maintain proper privilege management programs, due to the need for constant supervision and user-level updates. This increased maintenance need is why it's generally used by enterprise-level organizations or those in highly regulated industries.

So, if cost or internal support for this program is an issue with other non-InfoSec stakeholders, then consider tabling the discussion for this year. Then, pay closer attention to initial permissions at onboarding, and avoid granting anyone admin access permissions as a rule.

If more (qualified) requests for exceptions to your rules begin to occur, then gather these requests as support for a more tech-based privilege management solution. At some point, it will make economic sense to invest in a tool that can automate at least part of the process for you.

Defense Directory   Threat Actors   Tactical Index

Risk-based Patch and Vulnerability Management

Time to Functionality:

Days   Weeks   Months

Cost of Paid Tools (Entry to Robust Solutions)

$ $$ $$$ $$$$ $$$$$
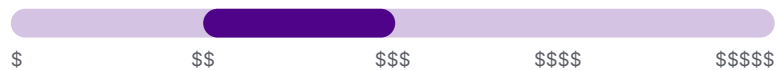
Description

These tools identify and prioritize fixes based on an organization's environment and needs – as well as roll out those patches! – instead of patching based on external vulnerability ratings of criticality or vendor severity.

How It Helps Defend

RBPM and RBVM tools help organizations prioritize the patches and security flaws that matter most for their devices and use case – which includes emphasizing the weaknesses and vulnerabilities that cybercriminals are using right now!

Arm Your People! – Justifying to Stakeholders

" Weren't we patching before? How is this different?

First, confirm that yes, your team was patching before, but remind your stakeholder of the fire drills that happen all the time. Wouldn't they like to avoid the emergencies due to headlines? RBVM and RBVM can proactively identify and patch the headlines that matter, respectively, before hackers come to you.

Then, explicitly reference the threat actor Defense Plays for those who have attacked organizations like yours, to show point-by-point where patching exploited or older vulnerabilities could have stopped hacker attacks early.

Finally, emphasize that you can't do this sort of patching manually. Only RBPM and RBVM tools can automatically figure out which exploits matter to your unique threat environment – and determine if your devices and data are protected!

" Why should we pay for this tool when there are free auto-patch software versions out there?

Point out that risk-based vulnerability management tools can impact multiple points of contact for threat actors throughout this book, so investments in RBVM and RBPM tools – one to prioritize, and the other to roll out patches – can prevent multiple points of attack throughout a hack, even if you don't know there's a hacker in the system.

Security Program Audits

Time to Functionality:

Days   Weeks   Months

Cost of Paid Tools (Entry to Robust Solutions)

$ $$ $$$ $$$$ $$$$$
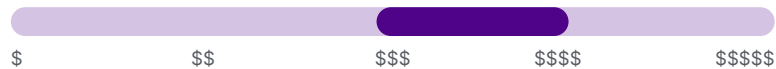
Description

Security Program Audits cover a wide range of services, but are generally summarized as third-party consultants or analysts who ensure cybersecurity solutions and programs are working; that environments and roles are still copacetic; and can determine if adjustments are needed. Penetration testing and employee phishing training can fall in this category.

How It Helps Defend

Frankly, it's very difficult for someone involved in any program or project to see its flaws. In many cases, an external security audit by a trusted provider is the only way you're going to know if your security program is actually working the way you've designed.

Deep audits may also flush out oddities or dormant intrusions by either internal threats or external hackers. An audit can also clean up loose ends and random details that haven't been reconciled or realigned to their current roles.

Arm Your People! – Justifying to Stakeholders

Didn't we just do an audit? Why pay for another one?

Audits should be completed more often for high-risk environments, partners and vendors. The more connected an environment is to mission-critical systems or to known targets of threat actors – such as a government agency or military contractor – the more likely it is that a hacker is trying to access the environment.

Frequent audits may also catch a lurking hacker who is gathering information before the attack is properly launched. Early identification of especially savvy threat actors can save your organization millions in lost data, reputation and legal expenses.

Defense Directory   Threat Actors   Tactical Index

Strategic Automation
specifically Alerts & Permission Requests

Time to Functionality:

Days   Weeks   Months

Cost of Paid Tools (Entry to Robust Solutions)

$ $$ $$$ $$$$ $$$$$
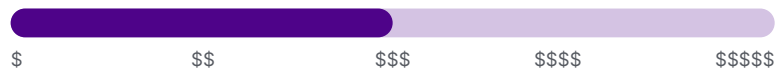
Description

In this context, we're discussing automated alerts of unwanted or unexpected activity, such as odd or out-of-place permission requests. Automation can also help facilitate day-to-day activities for general security programs.

How It Helps Defend

A single event log could go unnoticed by even the most detail-oriented security professional. However, that same event could trigger an alert threshold to inform the correct remediation team and automatically begin a seamless process of analysis and remediation.

As threats become more complex and as the responsibilities of the InfoSec team expand, automation can help overtaxed and impossible-to-hire-for security teams accomplish their missions without sacrificing the safety of the company.

Arm Your People! – Justifying to Stakeholders

Why pay for automation tools?

Often, paying for more automated solutions is cheaper and more accurate than hiring more security professionals… if you can even find a qualified candidate for the role.

Frequently, automation is a key feature of other security tools. It can be a value-added benefit to justify selecting one tool or solution over another.

We tried automation before, and it broke everything.

Emphasize to nervous stakeholders that automation is not a replacement for a human assessment, and will not be rolled out without thought, testing or care to disrupt business processes.

To that end, when making your request, list out exactly what your automation will and won't do, to set expectations and calm nerves across the board.

Why do we still submit tickets for access requests? ("Can we automate <service>?")

While automation can help with some of the administrative overhead, hackers can and will take advantage of completely automated systems.

For example, hackers could trick a completely automated access request process to gain higher permissions and reach more of the network. A human check can catch and stop that escalation.

User Access Control

Time to Functionality:

Days — Weeks — Months

Cost of Paid Tools (Entry to Robust Solutions)

$ — $$ — $$$ — $$$$ — $$$$$
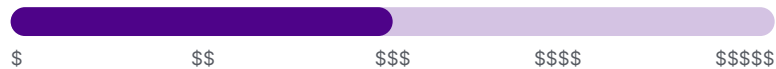
Description

User access control tools help proactively manage which employees and their job functions need access to which parts of the network and applications for their jobs. These tools also help retire access to previous permissions, as duties and roles change over time.

How It Helps Defend

Even if a hacker gained the credentials from an average employee, user access controls only allow that hacker to access what that employee could – not every possible file or data server. User access controls can also alert to unusual requests for access or attempts to break in, offering early warnings of lateral movement from previously unsensed hackers.

Arm Your People! – Justifying to Stakeholders

" Why does user access control cost so much?

Generally speaking, user access control tools are a "pay per seat" model. So, the bigger your organization gets, the more it will cost overall – and you'll need to plan changes to the budget allocation every year, as well, depending on how your organization plans to grow or consolidate.

Try reframing the ask in terms of an insurance per individual. Would the stakeholder be willing to pay $X per person, to avoid the risk of an average employee accidentally leaving their laptop credentials out and laying bare all of your intellectual property and customer records – even if they don't need access to that information?

" I don't have access to what I need anymore!

Try to make the process for your non-InfoSec stakeholders to submit change permission requests as simple and intuitive as possible.

Remind your team to be as patient as they can with any complaints – especially at the start! You can minimize many of these complaints by proactively including leads from all departments in the implementation process as project-consultants, telling you who needs access to which applications and their general workflows.

User Training & Education

Time to Functionality:

Days   Weeks   Months

Cost of Paid Tools (Entry to Robust Solutions)

$ $$ $$$ $$$$ $$$$$
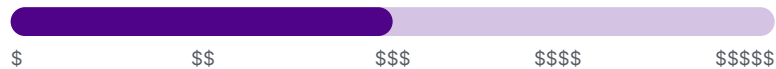
Description

Security training and education for the average non-InfoSec employee can run from basic training modules, to involved tabletop exercises and immersive simulations.

How It Helps Defend

Humans are the weakest link in any security chain. All the technology in the world cannot always prevent security accidents triggered by the most well-meaning of individuals. Training helps empower employees to take responsibility for their own cybersecurity, strengthening their own understanding and hardening the overall organization's security environment.

Arm Your People! – Justifying to Stakeholders

How can we implement training effectively?

Incentivize the average non-InfoSec individual to use their training by making a point to inform employees of attacks they, personally, helped prevent, such as when they report a phishing attack.

You can also help enforce healthy security protocols by subsidizing password managers.

As a rule, try not to punish employees for non-compliance. Instead, deliberately highlight and praise compliant behavior to make security a shared responsibility.

Why does user security training costs so much?

Effective user training is usually interactive with high-quality production – sometimes even custom scripts! These training modules are difficult to create, and so can be rather expensive.

However, the more interactive and relevant a user perceives their training to be, the greater participation and the better knowledge retention tends to be – which means they can actually use their security education when it matters the most.

Defense Directory   Threat Actors   Tactical Index

Web-based Content Restrictions

Time to Functionality:

Days — Weeks — Months

Cost of Paid Tools (Entry to Robust Solutions)

$ — $$ — $$$ — $$$$ — $$$$$
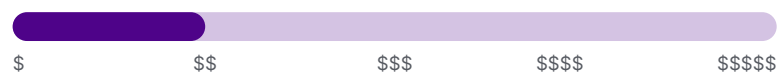
Description

These tools restrict what users can view or access online, while working from a protected work device.

How It Helps Defend

Threat actors and other hackers can route data and material through online applications. If you limit exposure to the internet, then you're limiting exposure to other threats – including possible malware and outside network intrusions that could otherwise "hide" in web traffic.

Arm Your People! – Justifying to Stakeholders

Why should we buy a tool that restricts web content?

Typically, this sort of tool is implemented in highly regulated, on-site environments, due to the complexity of the implementation – balancing restrictions of distracting or dangerous potential online content with actual, work-related online needs – and the growing popularity of remote work.

These organizations often include government facilities, hospitals, call centers and even banks with their ATMs.

However, if your organization wishes to move into highly regulated verticals, such as finance, health or government, then more restrictive tools may be worth the investment.

You may also see a boost in productivity – though be careful how you pitch this perk. Productivity will only be improved if employees can still access the content and resources they need to do their job, as well as distracting sites blocked during business hours.

Defense Directory   Threat Actors   Tactical Index

Featured 2022 Threat Actors

While there were quite a few cybersecurity incidents throughout 2022, driven by a wide variety of different criminal groups and motivations, we've selected four drastically different named threats to feature here.

Each of these groups will provide ample, relevant examples to help you push forward your strategic cybersecurity goals for 2023 – no matter what you're striving to accomplish.

ivanti | **CSW** Cyber SecurityWorks

Featured 2022 Threat Actors

In This Section

ALPHV

The ALPHV group – also known as "BlackCat" and the latest public iteration of BlackMatter and DarkSide hacker gangs – is a prime example of a cybercriminal gang responsible for creating, selling and deploying a "ransomware as a service" model, or RaaS.

What is RaaS, and why should your stakeholders care?

RaaS is basically an organization that profits in part from selling hacking software packages on the Dark Web or through various brokers.

With a little strategic social engineering to get a foothold in a target's computer system or network through compromised credentials, RaaS locks up any critical files unless the victim agrees to pay a ransom in exchange for a digital key.

As the creator of the original software, ALPHV charges a percentage of any collected ransom fee without any additional dirty work. (That said, the gang can and does attack select targets directly, collecting 100% of the ransom fee.)

The difference with RaaS from ordinary ransomware is twofold:

1 By packaging and selling the ransomware software, ALPHV and other RaaS providers write code on behalf of other criminals who can't (or don't want to) code – exponentially expanding the risk of potential cyberattacks within the landscape.

And, if hackers don't need to know how to write their own code to hack someone, then anyone with bad intentions becomes a cyberthreat.

2 Nation-state threat actors such as Nobelium use "off the shelf" hacks such as BlackCat's RaaS as part their espionage or attacks on foreign powers, speeding up attacks and disguising their involvement by using others' code while keeping their own secret hacks for more valuable targets.

While the adoption and expansion of RaaS as a Dark Web "business model" continues to drive an incredible uptick in attacks at all sorts of organizations, businesses and government agencies, it also presents an opportunity for savvy security teams.

Why? Because if many hackers use the same or similarly sourced "off the shelf" exploits by using the same or similar ransomware, then just a few preventative measures can prevent a wide swath of attacks.

ALPHV Stat Sheet

Aliases:

BlackCat	Noburus
ALPHV	AlphaVM
ALPHA	

Motive:

Criminal / Financial

Threat Type:

Ransomware as a Service Gang
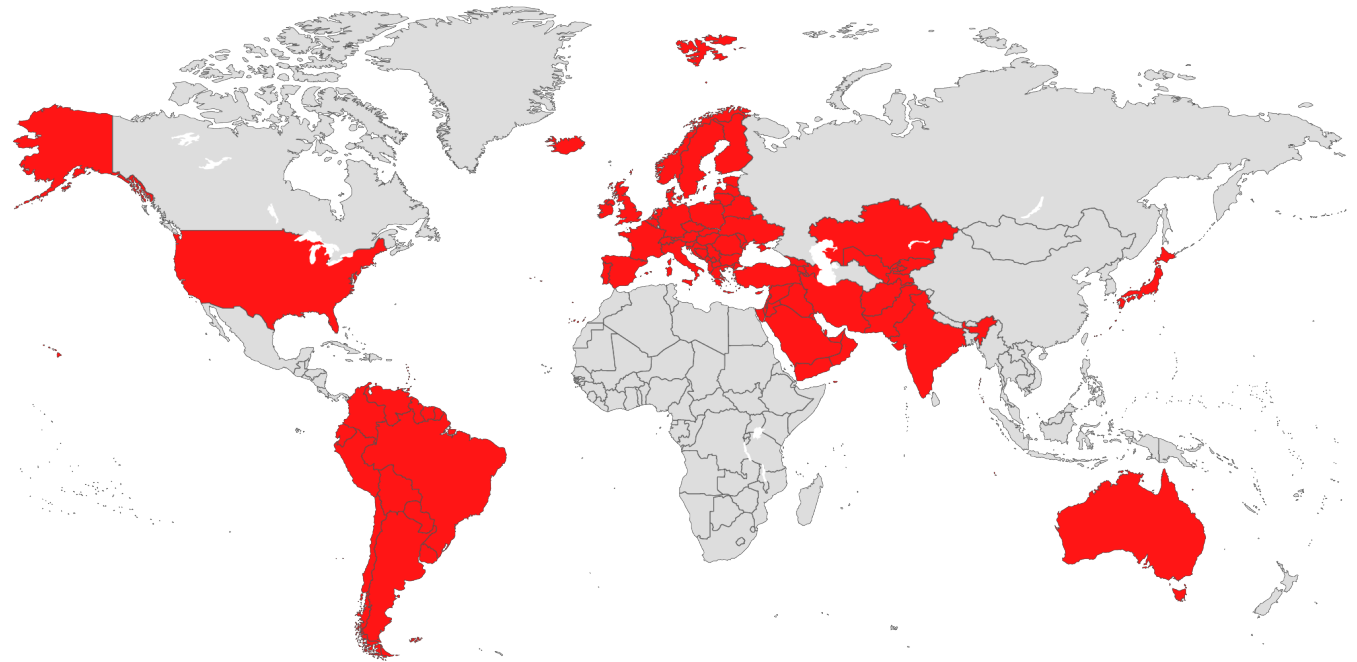
Affiliations and Associations:

Russia	FIN12
Ryuk	FIN7
Revil	Conti
DEV-0504	BlackMatter
DEV-0237	DarkSide

Favorite Exploits:

CVE-2016-0099	CVE-2021-34473
CVE-2019-7481	CVE-2021-34523
CVE-2021-31207	

Known Targeted Regions:

Australia	Japan
Austria	Middle East
Europe	South America
Germany	Switzerland
India	USA
Italy	

Organization Impact of Select ALPHV Attacks

"

The temporary outage of its IT services [...] impacted the operations of its logistics centers and client service activities.

December 23, 2021:
Moncler | Fashion / Retail | Milan

"

"Terminals are operating with limited capacity and have declared force majeure [an external, unavoidable and unforeseeable event]."

"It affects 233 fuel stations in northern Germany. It is probably possible to pay in cash."

January 29, 2022: Oiltanking + Mabanaft | Logistics | Germany

"We assume that of the 3,000 IT workstations affected, the first will be available again [four days after the attack.] [...] Because one is dependent on the IT systems, the administration is in emergency mode."

May 14, 2022: Carinthia | Government | Austria

"There is a possibility that customer information [...] was included in the [accessed] servers and PCs, and we are currently identifying [...] the existence of leakage, scope of the damage, and investigating the cause."

July 3, 2022: Bandai Namco | Entertainment | Japan

"We anticipate buildings to still be closed Monday with no definite time frame of reopening. [...]

We do understand that we are very vulnerable."

August 17, 2022: Fremont County | Government | USA

"[The IT] staff there is literally working around the clock to resolve this [attack]. I really feel for the colleagues there who are just putting in a Herculean lift to get us fully back and functional."

March 7-11, 2022: North Carolina A&T State University Education | USA

"Asked if data was encrypted or copied by [ALPHV], a spokesperson said the firm will not go beyond the statement."

May 31, 2022: CMC Electronics | Military / Aerospace Canada

"As our systems have been inaccessible for days, we are [working] hard to catch up with the backlog that has arisen."

July 22-23, 2022: Creos | Energy | Luxembourg

ivanti | CSW Cyber SecurityWorks

Defense Directory   Threat Actors   Tactical Index

An ALPHV Cyberdefense Strategy:
How to Help Stop ALPHV Attacks Before a Ransom Request

Enter network through compromised credentials.

Stopping hackers before they enter the network is the easiest, cheapest and fastest way to protect every business unit without disrupting operations.

▸ EDR
▸ Restrict Web-based Content
▸ Antivirus / Malware
▸ Anti-Phishing on Mobile
▸ User Training & Education
▸ Passwordless MFA
▸ User Access Control
▸ Application Control
▸ Device Hygiene & Management
▸ Security Program Audits
▸ Strategic Automation
▸ Configuration Management

Map system information and network

When intruders can't move freely or easily in the network, they can't find important data or vulnerabilities – mitigating major business impact.

▸ Risk-based Patch & Vulnerability Management
▸ Device & Network Segmentation
▸ Device Hygiene & Management
▸ Asset Reconciliation
▸ Secure Access Protocols
▸ Network Segmentation
▸ Privilege Management
▸ Strategic Automation
▸ Configuration Management

Create victim-specific ransomware based on unique "holes" or exploits.

If cybercriminals can't launch their ransomware, then they can't lock or steal data for ransom.

▸ Risk-based Patch & Vulnerability Management
▸ Application Control
▸ User Access Control
▸ Privilege Management
▸ Device Hygiene & Management
▸ Strategic Automation

Stop security programs from blocking the ransomware attack or removal of data.

Unusual behavior alerts can signal the opening stages of a ransomware attack before business shutdown or ransom demands.

▸ Application Control
▸ Strategic Automation
▸ User Access Control

Encrypt files and data exfiltration (removal or copying from the system) to create leverage against victim.

If the hackers can't steal or lock data, then they have little leverage to demand a ransom.

▸ Malicious Encryption Detection & Isolation
▸ Device and Network Segmentation
▸ Restricting Web-based Content

Too late for proactive prevention; shift to "disaster recovery" mode.

ivanti | CSW Cyber SecurityWorks

Defense Directory   Threat Actors   Tactical Index

APT29

The infamous hackers who leaked the Democratic National Committee's internal emails and documents, APT29, or "Nobelium," is a cyber organization connected to Russia's foreign intelligence service dedicated to espionage and intelligence activities.

"APT" stands for "advanced persistent threat." This designation usually describes a nation- or state-sponsored threat group which can penetrate an organization's network and lurk for months – even years – before either detection or attack.

Why should your stakeholders care about APT29 if you're not a government agency?

As soon as non-InfoSec stakeholders hear that the latest threat actor making headlines this week is part of Russian intelligence, they may want to dismiss the threat altogether.

"Why would APT29 care about us?" they might say. "We're not a government agency! We're not part of a war effort!"

Enter: the small world problem.

Many social network research studies – from doctoral dissertations to Meta's Facebook research to meme games featuring actor Kevin Bacon – have examined connections between one relationship to the next in populations of various sizes. The average "distance" from any starting point to the final "destination" seems to be around three to four connections.

Now, let's extend this hypothetical scenario to your push for a proactive cybersecurity strategy.

While your organization might not be a government agency or an activist non-profit making trouble for Russia, it's not unheard of for threat actors to target connections to their end goals – or connections-of-connections-of-connections via supply chain attacks – to affect crisis and extract information.

For example, take the famous SolarWinds incident – an APT29 cyberattack from 2020.

APT29 hackers didn't target government agencies or critical infrastructure organizations directly. Instead, they infected the software vendor-of-a-contractor, a network monitoring software platform, to then install backdoors on some 18,000 customers through a routine software update... which included government users.

Not all 18,000 customers were targeted by APT29, but all were hacked – and all were made vulnerable when they got caught up in an underground cyberwar between powerful nations.

So, if any of your non-InfoSec stakeholders want to push back against preparing against APT29 or any other advanced persistent threat group because you're "neutral" or a non-combatant, then play the 6 Degrees of Separation game as a tabletop exercise or workshop activity.

But this time, play through your organization's connections to Russia.

Statistically speaking, your organization is much closer to being an APT29 target – or target for any other APT group – than non-InfoSec stakeholders would like to believe.

Defense Directory   Threat Actors   Tactical Index

APT29 Stat Sheet

Aliases:

Nobelium	Cozy Bear	UNC-1151
YTTRIUM	CozyDuke	Cloaked Ursa
The Dukes	UAC-0113	

Motive:

Espionage / Covert Operations

Threat Type:

Advanced Persistent Threat / APT

Affiliations and Associations:

Russia	APT28	Actinium	Blue Athena
Conti	Strontium	Bromine	SolarStorm
ALPHV	Iridium	Krypton	Tsar Team
Fighting Ursa	DEV-0586	StellarParticle	Minidionis

Favorite Exploits:

CVE-2009-3129	CVE-2019-17026	CVE-2020-14882
CVE-2014-1761	CVE-2019-19781	CVE-2020-4006
CVE-2015-164	CVE-2019-2725	CVE-2020-5902
CVE-2018-13379	CVE-2019-7609	CVE-2021-1879
CVE-2019-11510	CVE-2019-9670	CVE-2021-21972
CVE-2019-1653	CVE-2020-0674	CVE-2021-26855

Critical At-risk Industries:

Government	Media and	Healthcare
Military	Telecommunications	Higher Education
Energy	NGOs and Non-profits	Financial
IT	Transportation	Research / Think Tanks
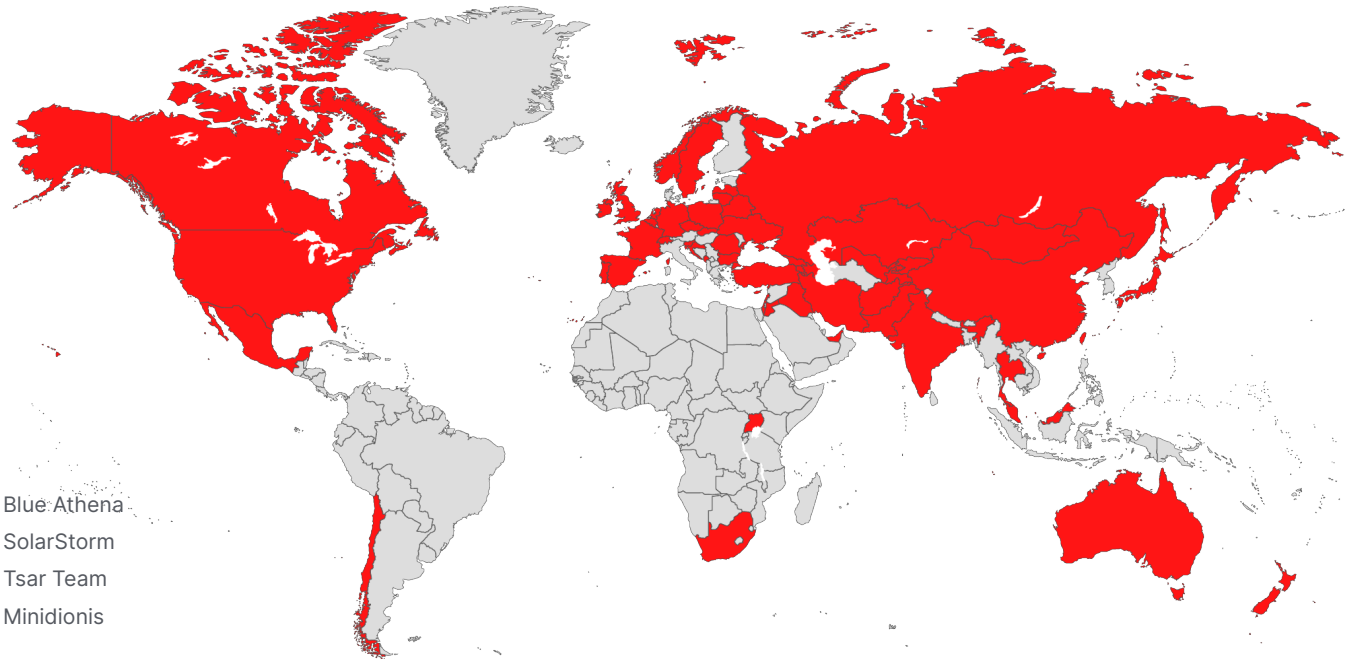
Known Targeted Regions:

Afghanistan	Chile	Iran	Lithuania	Poland	Switzerland
Armenia	China	Iraq	Luxembourg	Portugal	Tajikistan
Australia	Croatia	Ireland	Malaysia	Romania	Thailand
Azerbaijan	Cyprus	Israel	Mexico	Russia	Turkey
Belarus	Czech	Japan	Mongolia	Slovakia	UAE
Belgium	France	Jordan	Montenegro	Slovenia	Uganda
Brazil	Georgia	Kazakhstan	Netherlands	South Africa	UK
Bulgaria	Germany	Kyrgyzstan	New Zealand	South Korea	Ukraine
Canada	Hungary	Latvia	Norway	Spain	United States
Chechnya	India	Lebanon	Pakistan	Sweden	Uzbekistan

Defense Directory   Threat Actors   Tactical Index

Organization Impact of Select APT29 Attacks

"
The phishing emails sent by APT29 **masqueraded as administrative notices** related to various embassies and utilized legitimate but co-opted email addresses.

Attack Started January 17, 2022 – Announced April 28, 2022: Diplomatic Entities | Europe, Asia, North America

"These actors [including APT29] take advantage of **simple passwords, unpatched systems, and unsuspecting employees** to gain initial access before moving laterally through the network to establish persistence and exfiltrate data."

Attack Started January 2020 – Announced February 16, 2022: Cleared Defense Contractors | Military | USA

"Administrators found PCs locked and displaying a message demanding $10,000 in bitcoin, but the **machines' hard drives were irreversibly corrupted** when an admin rebooted them."

January 13, 2022: Government, Non-profit & IT Organizations | Ukraine

"Since early May, Cloaked Ursa [APT29] has continued to evolve their abilities to **deliver malware using popular online storage services**[, including] DropBox and Google Drive services."

Attack Started May 2022 – Announced July 5, 2022: Foreign Embassies | Portugal and Brazil

"As early as May 2021, Russian state-sponsored cyber actors **took advantage of a misconfigured account set to default MFA protocols** at a non-governmental organization (NGO), allowing them to enroll a new device for MFA and access the victim network."

Attack Started May 2021 – Announced March 15, 2022: Non-government Organization | USA

"There is an increased potential for cyber attacks. These may have serious impact, **even for countries and organisations not directly targeted** [by cyber campaigns conducted by Russia]."

February 18, 2022: "Nationally Significant Organizations" New Zealand

"There has been a notable **continuation of the use of [publicly] available commodity malware**, showing UAC-0113 [APT29] adapting its operations with a willingness to use a variety of tooling."

Announced September 19, 2022: Government and Private Sector | "Multiple Geographic Regions"

ivanti | **CSW** Cyber SecurityWorks

An APT29 Cyberdefense Strategy:
How to Break APT29 Attacks Before Detection or Deletion

Enter network through phishing campaigns or via compromised supply chain vendors.

Stopping hackers before they enter the network is the easiest, cheapest and fastest way to protect every business unit without disrupting operations.

▶ EDR
▶ Restrict Web-based Content
▶ Antivirus / Malware
▶ Anti-Phishing
▶ User Training & Education
▶ Passwordless MFA
▶ User Access Control
▶ Application Control
▶ Device Hygiene & Management
▶ Security Program Audits
▶ Strategic Automation
▶ Configuration Management

Access admin profiles and / or intercept authentication packets to elevate hacked permissions.

Limiting intruders' ability to elevate credentials helps prevent data theft and extortion.

▶ User Access Control
▶ Privilege Management
▶ Configuration Management
▶ Security Program Audits
▶ User Training & Education

Map network for useful information and weaknesses.

When intruders can't move freely or easily in the network, they can't find important data or vulnerabilities – mitigating major business impact.

▶ Risk-based Patch & Vulnerability Management
▶ Device & Segmentation
▶ Device Hygiene & Management
▶ Asset Reconciliation
▶ Secure Access Protocols
▶ Network Segmentation
▶ Privilege Management
▶ Strategic Automation
▶ Configuration Management

Wait, exfiltrating data and increasing foothold against defenses if discovered in part by erasing logs.

Unusual behavior alerts can signal the opening stages of a ransomware attack before business shutdown or ransom demands.

▶ Security Program Audits
▶ EDR
▶ Restricting Web-based Content
▶ Strategic Automation
▶ Malicious Encryption Detection & Isolation

Attack on command for greatest confusion and impact.

Too late for proactive prevention; shift to "disaster recovery" mode.

$

ivanti | CSW Cyber SecurityWorks

Defense Directory   Threat Actors   Tactical Index

Conti

For anyone in cybersecurity following the latest ransomware news, "Conti" is a familiar name. Another threat actor associated with – if not actively sponsored by – Russia, the ransomware-as-a-service group made public headlines in February 2022 by announcing its "full support of the Russian government" after its Ukrainian invasion.

However, since internal malcontents published the organization's affiliate training playbook and external security researchers leaked its internal documents on Twitter, "Conti" as a single criminal organization seems to have dissolved completely.

With a lack of immediate news to pressure them into action, non-InfoSec stakeholders may question your cybersecurity strategy if you bring up Conti ransomware prevention – but you know that's a red herring distraction from the real threat.

If Conti is gone, why should stakeholders care about preventing previous attacks?

Frankly, Conti had a reputation problem for a while – ironically, due to its own poor operational security and internal morale!

Its downhill slide started with the leaked training playbooks for affiliate Conti ransomware members. The final nail in the coffin came when an anonymous Ukrainian IT specialist broke into the gang's network to leak years of internal material.

But, just because Conti is "dead," doesn't mean its hackers aren't still operating or that its code is suddenly defunct.

After all, Conti had an extensive affiliate organization, who were clearly trained on how to use the written ransomware code and techniques that still present themselves as a threat to any organization with the vulnerabilities still present.

And, it's not like the hackers, programmers and social engineers at the Conti organization itself were arrested or died.

In fact, two full months after Conti shut down its servers, the United States State Department released a new video highlighting its $10 million reward for information leading to the arrest of any "Conti" hackers.

Recently, cybersecurity researchers and analysts have seen Conti-style tactics from other cybercriminal gangs, including:

- BlackByte
- Karakurt
- BlackBasta
- HelloKitty
- AvosLocker
- Hive
- ALPHV – and others!

By studying previous Conti incidents, today's proactive organizations can prevent a multitude of similar attacks run by smaller threat actors using Conti's tactics.

Defense Directory   Threat Actors   Tactical Index

Conti Stat Sheet

Aliases:
No longer available

Motive:
Criminal / Financial

Threat Type:
Ransomware-as-a-Service (RaaS)

Affiliations and Associations:

Russia	BlackBasta	Hive
BlackByte	HelloKitty	AvosLocker
Karakurt	ALPHV	Wizard Spider

Critical At-risk Industries:

Government	Hospitality	Education
Finance	Finance	Food & Beverage
Energy	Technology	Retail & eCommerce
Manufacturing	Healthcare	

Favorite Exploits:

CVE-2017-0143	CVE-2018-13379	CVE-2021-44228	CVE-2019-1069	CVE-2019-1388	CVE-2021-21972
CVE-2017-0144	CVE-2020-0796	CVE-2015-2546	CVE-2019-1129	CVE-2019-1405	CVE-2021-21985
CVE-2017-0145	CVE-2020-1472	CVE-2016-3309	CVE-2019-1130	CVE-2019-1458	CVE-2021-22005
CVE-2017-0146	CVE-2021-1675	CVE-2017-0101	CVE-2019-1215	CVE-2020-0609	CVE-2021-26855
CVE-2017-0147	CVE-2021-31207	CVE-2018-8120	CVE-2019-1253	CVE-2020-0638	
CVE-2017-0148	CVE-2021-34473	CVE-2019-0543	CVE-2019-1315	CVE-2020-0688	
CVE-2018-12808	CVE-2021-34523	CVE-2019-0841	CVE-2019-1322	CVE-2020-0787	
CVE-2018-13374	CVE-2021-34527	CVE-2019-1064	CVE-2019-1385	CVE-2021-1732	
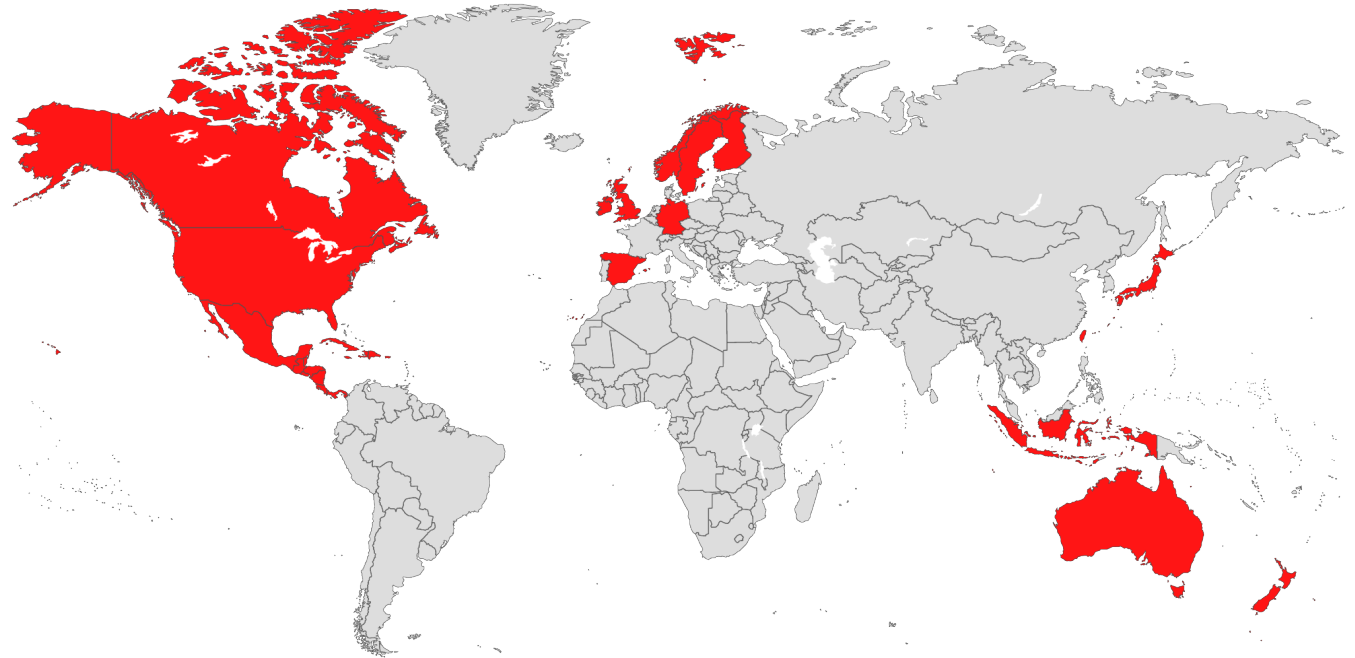
Known Targeted Regions:

Australia	New Zealand
Canada	Scandinavia
Costa Rica	Spain
Germany	Taiwan
Indonesia	United Kingdom
Ireland	United State
Japan	
Latin America	

ivanti | CSW Cyber SecurityWorks

Defense Directory   Threat Actors   Tactical Index

Organization Impact of Select Conti Attacks

" Of the 65,000 computers in Delta [Electronic]'s network, about 1,500 servers and about 12,000 computers are encrypted. [...] It has been nearly a week since the incident, and the Delta website has not yet been restored, and the impact of the loss may exceed expectations. "

January 21, 2022: Delta Electronics
Manufacturing | Taiwan

"[...] Conti had encrypted over 4,000 devices and 120 VMware ESXi servers belonging to Shutterfly. A private data leak page also showed samples of the data stolen from Shutterfly, which we are told included legal agreements, bank and merchant account info, [...] and what appears to be customer information, including the last four digits of credit cards."

Attacked December 3, 2021 – Reported December 26, 2021:
Shutterfly | Retail & eCommerce | United States

"At this stage we cannot safely process orders or dispatch goods. We have teams working through the resolution, but it is unknown when this will be resolved."

January 28, 2022: KP Snacks | Food & Beverage
United Kingdom

"Christian Rucavado, executive director of Costa Rica's Exporters Chamber, said the attack on the customs agency had collapsed the country's import and export logistics. He described a race against the clock for perishable items waiting in cold storage and said they still didn't have an estimate for the economic losses."

April 18, 2022: Finance, Labor and Social Security Ministries
Government | Costa Rica

"BI is aware of a ransomware hack last month. We are aware that we have been hit by a cyber attack. This is a crime, it is real, and we are exposed to it."

Attacked December 2021 – Reported January 20, 2022:
Bank of Indonesia | Finance | Indonesia

"To safeguard customer assets, remote access from Nordex Group IT infrastructure was disabled for turbines under contract. [... The] company is continuing to restore its IT systems such as to enable business continuity and resume normal operations as soon as reasonably practicable."

March 31, 2022: Nordex | Manufacturing / Energy | Germany

DISBANDED by JUNE 2022

ivanti | CSW Cyber SecurityWorks

Defense Directory   Threat Actors   Tactical Index

A Conti Legacy Cyberdefense Strategy:
How to Break Conti-styled Attacks Before the Ransom Request

Enter network through phishing campaigns, weak firewalls and / or badly configured internet-connected servers or devices.

Stopping hackers before they enter the network is the easiest, cheapest and fastest way to protect every business unit without disrupting operations.

- ▶ EDR
- ▶ Restrict Web-based Content
- ▶ Antivirus / Malware
- ▶ Anti-Phishing on Mobile
- ▶ User Training & Education
- ▶ Passwordless MFA
- ▶ User Access Control
- ▶ Application Control
- ▶ Device Hygiene & Management
- ▶ Security Program Audits
- ▶ Strategic Automation
- ▶ Configuration Management

Gain admin privileges on hacker user accounts, proactively disguising activity as legitimate.

Limiting intruders' ability to elevate credentials helps prevent data theft and extortion.

- ▶ User Access Control
- ▶ Privilege Management
- ▶ Configuration Management
- ▶ Security Program Audits
- ▶ User Training & Education

Map network for strategic information and weaknesses.

When intruders can't move freely or easily in the network, they can't find important data or vulnerabilities – mitigating major business impact.

- ▶ Risk-based Patch & Vulnerability Management
- ▶ Device & Segmentation
- ▶ Device Hygiene & Management
- ▶ Asset Reconciliation
- ▶ Secure Access Protocols
- ▶ Network Segmentation
- ▶ Privilege Management
- ▶ Strategic Automation
- ▶ Configuration Management

Exfiltrate data to hold for extortion.

If the hackers can't steal or lock data, then they have little leverage to demand a ransom.

- ▶ Security Program Audits
- ▶ EDR
- ▶ Restricting Web-based Content
- ▶ Strategic Automation
- ▶ Malicious Encryption Detection & Isolation

Launch ransomware and make extortion demands, with possible DDoS attack to pressure for payment.

⚠

Too late for proactive prevention; shift to "disaster recovery" mode.

Defense Directory   **Threat Actors**   Tactical Index

Lapsus$

Like Conti, everyone thought Lapsus$ was finished with the City of London Police's arrest of their ringleader – a 16-year-old hacker with autism going by "White" or "Breachbase" – in March 2022.

But, just a few months later, big corporations pinned their old breaches on the thought-defunct gang. And then, altogether new infiltrations at major technology companies grabbed the headlines!

Like Conti, this seemingly spontaneous resurrection of Lapsus$ as a cybercriminal threat can help you remind your non-InfoSec stakeholders that even "dead" cyberthreats should still be defended against.

However, we included Lapsus$ as the group represents a wildly different type of motivation for attack and infiltration method.

See, Lapsus$ doesn't seem to be primarily motivated by money, though they certainly ransom information and blackmail organizations into forking over millions.

Instead, Lapsus$ hackers appear to attack out of curiosity – "Can I even do this?" – and that age-old young person's drive for attention by any means necessary.

Why should a bunch of teen hackers worry your stakeholders?

To convince your stakeholders on why Lapsus$ attacks are worth investing in to avoid attack, you'll first need to illustrate just how different an infiltration and attack method these teenagers leveraged.

After all, these hackers didn't have a ton of money or connections, like our other featured threat actors. They didn't have time to dedicate to a criminal enterprise, like adult hackers whose full-time job was making money from criminal activity.

Instead, Lapsus$ hackers leveraged the tools at their disposal to infiltrate organizations: social media.

On their public Telegram channel, Lapsus$ announced that they were looking for initial logins

and other hackable information on major companies and organizations. They'd be willing to trade cryptocurrencies for the information, if the informant wanted to be paid.

And, disgruntled employees did seem to take advantage of their offer.

In the weeks and months that followed the initial Telegram post, several major organizations publicly announced breaches they attributed to the Lapsus$ gang.

Once they gained access to an organization, they would move laterally through the system as far as they could – going so far as to internally phish other employees and IT departments using the compromised credentials. They could access shared drives, lurk in the background of meetings and discover unencrypted password docs.

Then, Lapsus$ hackers could export data, delete it and watch the mayhem unfold from the inside. They could even deliver ransom demands through internal communication channels!

> **If your employee morale is critically low and your non-InfoSec stakeholders don't take ownership of their own roles in cybersecurity, then they represent grave "insider threats" to your organization's operational security – both inside and out – exemplified by Lapsus$ cyberattack patterns.**

Defense Directory   Threat Actors   Tactical Index

Lapsus$ Stat Sheet

Aliases:
N/A

Motive:
Hacktivists, Financial

Threat Type:
General Hackers

Affiliations and Associations:
UNC2447
Yanluowangr

Critical At-risk Industries:
Entertainment
Technology

Favorite Exploits:

CVE-2021-34484	CVE-2021-44957	CVE-2021-45325	CVE-2021-34484
CVE-2018-13379	CVE-2021-45326	CVE-2021-44956	CVE-2022-21919
CVE-2020-12812	CVE-2021-45328	CVE-2021-34473	CVE-2022-26904
CVE-2020-23852	CVE-2022-0510	CVE-2021-26858	CVE-2021-34484
CVE-2021-26857	CVE-2022-21702	CVE-2021-26855	
CVE-2021-31207	CVE-2022-0139	CVE-2020-23705	
CVE-2021-44864	CVE-2021-45327	CVE-2019-5591	
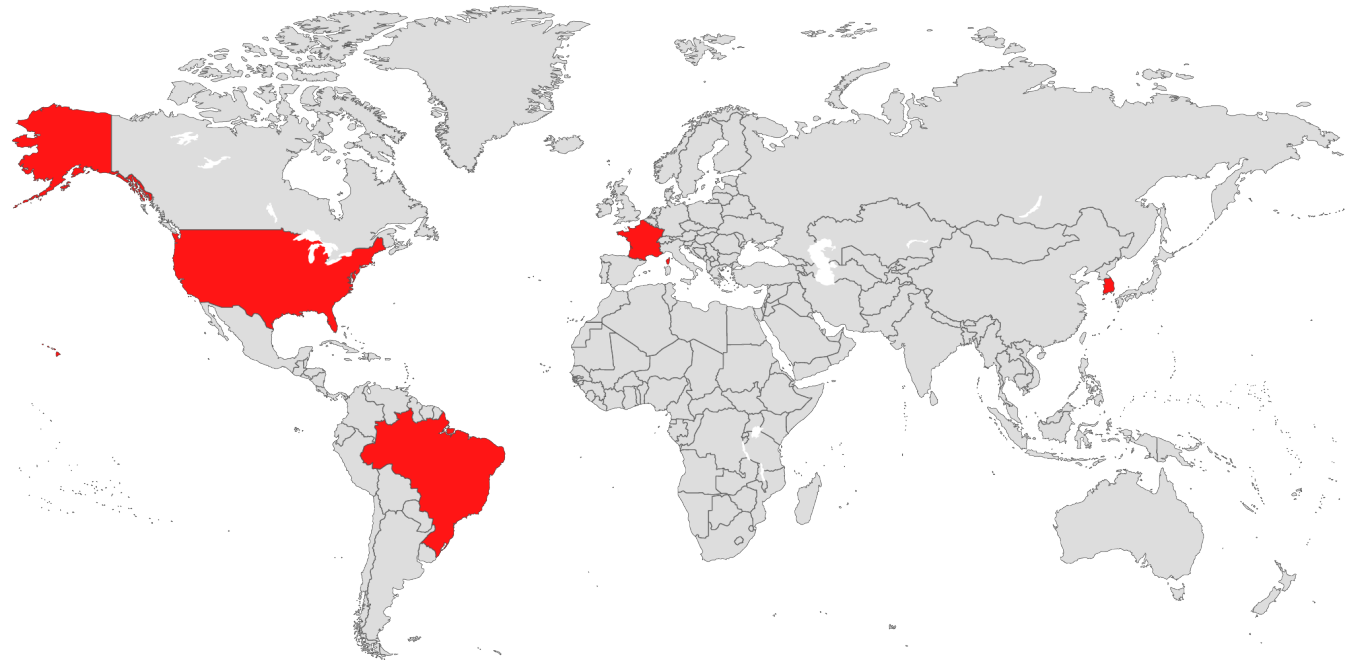
Known Targeted Regions:

Brazil
France
South Korea
United States

Defense Directory   Threat Actors   Tactical Index

Organization Impact of Select Lapsus$ Attacks

"

The attacker then repeatedly tried to log in to the contractor's Uber account. Each time, the contractor received a two-factor login approval request, which initially blocked access. Eventually, however, the contractor accepted one, and the attacker successfully logged in.

"

September 15, 2022: Uber | Technology United States

"I am greatly disappointed by the long period of time that transpired between our notification to [firm] and the issuance of the complete investigation report. Upon reflection, once we received the [firm's] summary report we should have moved more swiftly to understand its implications."

January 2022: Okta | Technology | United States

"According to our initial analysis, the breach involves some source codes relating to the operation of Galaxy devices but does not include the personal information of our consumers or employees."

Announced March 3, 2022: Samsung | Electronics / Manufacturing | South Korea

"On September 11, 2022, the bad actors who previously published a list of file names from this security incident to the dark web, posted the actual contents of the same files to the same location on the dark web."

Attacked May 24, 2022 – Reported August 10, 2022: Cisco Electronics / Manufacturing | United States

"We are aware that the threat actor [Lapsus$] took employee credentials and some Nvidia proprietary information from our systems and has begun leaking it online."

February 23, 2022: Nvidia | Electronics / Manufacturing United States

"When posting the torrent, Lapsus$ said it contained 90% of the source code for Bing and approximately 45% of the code for Bing Maps and Cortana."

March 20, 2022: Microsoft | Technology | United States

"We recently suffered a network intrusion in which an unauthorized third party illegally accessed and downloaded confidential information from our systems, including early development footage for the next Grand Theft Auto."

September 19, 2022: Rockstar Games | Entertainment United States

Your Lapsus$ Cyberdefense Strategy:
How to Break Lapsus$ Attacks Before Vandalism or Deletion

Enter network through insider threat's credentials, as well as employees' personal accounts as "backdoor" to employer network.

Stopping hackers before they enter the network is the easiest, cheapest and fastest way to protect every business unit without disrupting operations.

▶ User Access Control
▶ Privilege Management
▶ Security Program Audits
▶ Application Control
▶ Passwordless MFA
▶ Network Segmentation
▶ User Training & Education
▶ Strategic Automation

Search for exposed credentials in open shared databases or by social engineering internal attacks from within.

Limiting intruders' ability to change or elevate credentials helps prevent data theft and extortion.

▶ User Access Control
▶ Privilege Management
▶ Security Program Audits
▶ Application Control
▶ Passwordless MFA
▶ Network Segmentation
▶ User Training & Education
▶ Strategic Automation

Exfiltrate data for either notoriety (proof of hack) or for future extortion.

If the hackers can't steal data, then they have little leverage to demand a ransom.

▶ Restricting Web-Based Content
▶ User Access Control
▶ Privilege Management
▶ Network Segmentation
▶ Application Control
▶ EDR
▶ Security Program Audits
▶ Strategic Automation
▶ Device Hygiene & Management

Begin extortion – possibly from the victim's own internal channels! – as organization begins incident response.

Too late for proactive prevention; shift to "disaster recovery" mode.

$

ivanti | CSW Cyber SecurityWorks

InfoSec Tactical Index

In This Section

InfoSec Tactical Index

ALPHV MITRE ATT&CK Map

1. Reconnaissance
T1595: Active Scanning
T1589: Gather Victim Identity Information
   T1589.001: Credentials

2. Resource Development
n/a

3. Initial Access
T1078: Valid Accounts
T1190: Exploit Public-Facing Application

4. Execution
n/a

5. Persistence
T1098: Account Manipulation

6. Privilege Escalation
T1548: Abuse Elevation Control Mechanism
   T1548.002: Bypass User Account Control

7. Defense Evasion
T1564: Hide Artifacts

8. Credential Access
T1003: OS Credential Dumping
   T1003.001: LSASS Memory
   T1003.004: LSA Secrets

9. Discovery
T1082: System Information Discovery
T1135: Network Share Discovery
T1018: Remote System Discovery
T1087: Account Discovery
   T1087.002: Domain Account
T1487: Domain Trust Discovery
T1057: Process Discovery
T1083: File & Directory Discovery

10. Lateral Movement
T1563: Remote Service Hijacking
   T1563.002: RDP Hijacking
T1570: Lateral Tool Transfer

11. Collection
T1005: Data from Local System

12. Command and Control
T1090: Proxy
   T1090.003: Multi-hop Proxy

13. Exfiltration
T1567: Exfiltration Over Web Service
   T1567.002: Exfiltration to Cloud Storage

14. Impact
T1486: Data Encrypted for Impact
T1489: Service Stop
T1490: Inhibit System Recovery

Defense Directory   Threat Actors   Tactical Index

APT29 MITRE ATT&CK Map

1. Reconnaissance

n/a

2. Resource Development

T1583: Acquire Infrastructure
  T1583.001: Domains
  T1583.006: Web Services
T1584: Compromise Infrastructure
  T1584.001: Domains
T1587: Develop Capabilities
  T1587.001: Malware
  T1587.003: Digital Certificates

3. Initial Access

T1078: Valid Accounts
  T1078.002: Domain Accounts
T1133: External Remote Services
T1190: Exploit Public-Facing Application
T1195: Supply Chain Compromise
  T1195.002: Compromise Software
  Supply Chain
T1566: Phishing
  T1566.001: Spearphishing Attachment
  T1566.002: Spearphishing Link

4. Execution

T1047: Windows Management Instrumentation
T1204: User Execution
  T1204.001: Malicious Link
  T1204.002: Malicious File
T1053: Scheduled Task/Job
  T1053.005: Scheduled Task
T1059: Command and Scripting Interpreter
  T1059.001: PowerShell
  T1059.003: Windows Command Shell
  T1059.006: Python
T1203: Exploitation for Client Execution

5. Persistence

T1053: Scheduled Task/Job
  T1053.005: Scheduled Task
T1078: Valid Accounts
  T1078.002: Domain Accounts
T1098: Account Manipulation
  T1098.001: Additional Cloud
  Credentials
  T1098.002: Additional Email Delegate
  Permissions
T1133: External Remote Services
T1546: Event Triggered Execution
T1546.003: Windows Management
Instrumentation Event Subscription
T1546.008: Accessibility Features

6. Privilege Escalation

T1053: Scheduled Task/Job
  T1053.005: Scheduled Task
T1078: Valid Accounts
  T1078.002: Domain Accounts
T1484: Domain Policy Modification
  T1484.002: Domain Trust Modification
T1546: Event Triggered Execution
  T1546.003: Windows Management
  Instrumentation Event Subscription
  T1546.008: Accessibility Features
T1547: Boot or Logon Autostart Execution
  T1547.009: Shortcut Modification

7. Defense Evasion

T1027: Obfuscated Files or Information
  T1027.002: Software Packing
T1036: Masquerading
  T1036.004: Masquerade Task or
  Service
  T1036.005: Match Legitimate Name
  or Location
T1070: Indicator Removal on Host
  T1070.004: File Deletion
  T1070.006: Timestomp
T1078: Valid Accounts
  T1078.002: Domain Accounts
T1140: Deobfuscate/Decode Files or
Information
T1218: System Binary Proxy Execution
  T1218.011: Rundll32
T1484: Domain Policy Modification
  T1484.002: Domain Trust
  Modification
T1548: Abuse Elevation Control Mechanism
  T1548.002: Bypass User Account
  Control
T1550: Use Alternate Authentication Material
  T1550.003: Pass the Ticket
  T1550.004: Web Session Cookie
T1553: Subvert Trust Controls
  T1553.002: Code Signing
T1562: Impair Defenses
  T1562.001: Disable or Modify Tools
  T1562.002: Disable Windows Event
  Logging
  T1562.004: Disable or Modify System Firewall

8. Credential Access

T1003: OS Credential Dumping
  T1003.006: DCSync
T1005: Data from Local System
T1552: Unsecured Credentials
  T1552.004: Private Keys
T1555: Credentials from Password Stores
T1558: Steal or Forge Kerberos Tickets
  T1558.003: Kerberoasting
T1606: Forge Web Credentials:
  T1606.001: Web Cookies
  T1606.002: SAML Tokens

9. Discovery

T1016: System Network Configuration
Discovery
  T1016.001: Internet Connection
  Discovery
T1018: Remote System Discovery
T1057: Process Discovery
T1069: Permission Groups Discovery
T1082: System Information Discovery
T1083: File and Directory Discovery
T1087: Account Discovery
T1482: Domain Trust Discovery

10. Lateral Movement

T1021: Remote Services
  T1021.006: Windows Remote
  Management
T1550: Use Alternate Authentication Material
  T1550.003: Pass the Ticket
  T1550.004: Web Session Cookie

11. Collection

T1074: Data Staged
  T1074.002: Remote Data Staging
T1114: Email Collection
  T1114.002: Remote Email Collection
T1560: Archive Collected Data
  T1560.001: Archive via Utility

12. Command and Control

T1001: Data Obfuscation
  T1001.002: Data Obfuscation:
  Steganography
T1071: Application Layer Protocol
  T1071.001: Web Protocols
T1090: Proxy
  T1090.001: Internal Proxy
  T1090.003: Multi-hop Proxy
  T1090.004: Domain Fronting
T1095: Non-Application Layer Protocol
T1102: Web Service
  T1102.002: Bidirectional Communication
T1105: Ingress Tool Transfer
T1568: Dynamic Resolution

13. Exfiltration

T1048: Exfiltration Over Alternative Protocol
  T1048.002: Exfiltration Over
  Asymmetric Encrypted
  Non-C2 Protocol

14. Impact

n/a

ivanti | **CSW** Cyber Security Works

Defense Directory   Threat Actors   Tactical Index

Conti MITRE ATT&CK Map

1. Reconnaissance

T1595: Active Scanning

2. Resource Development

n/a

3.Initial Access

T1190: Exploit Public-Facing Application
T1566: Phishing
    T1566.001: Spearphishing Attachment
    T1566.002: Spearphishing Link
    T1566.003: Spearphishing via Service

4. Execution

T1072: Software Deployment Tools
T1203: Exploitation for Client Execution

5. Persistence

T1037: Boot or Logon Initialization Scripts
T1542: Pre-OS Boot
T1542.003: Bootkit
T1543: Create or Modify System Process
    T1543.001: Launch Agent
    T1543.002: Systemd Service
    T1543.003: Windows Service
    T1543.004: Launch Daemon
T1546: Event Triggered Execution
    T1546.001: Change Default File Association
    T1546.004: Unix Shell Configuration Modification
    T1546.008: Accessibility Features
T1547: Boot or Logon Autostart Execution
    T1547.006: Kernel Modules and Extensions
    T1547.009: Shortcut Modification
T1574: Hijack Execution Flow
    T1574.008: Path Interception by Search Order Hijacking
T1574.009: Shortcut Modification
    T1574.010: Services File Permissions Weaknesses
    T1574.011: Services Registry Permissions Weakness

6.Privilege Escalation

T1037: Boot or Logon Initialization Scripts
T1055: Process Injection
T1134: Access Token Manipulation
T1543: Create or Modify System Process
    T1543.001: Launch Agent
    T1543.002: Systemd Service
    T1543.003: Windows Service
    T1543.004 Launch Daemon
T1546: Event Triggered Execution
    T1546.001: Change Default File Association
    T1546.004: Unix Shell Configuration Modification
    T1546.008: Accessibility Features
T1547: Boot or Logon Autostart Execution
    T1547.006: Kernel Modules and Extensions
    T1547.009: Shortcut Modification
T1548: Abuse Elevation Control Mechanism
T1574: Hijack Execution Flow
    T1574.010: Services File Permissions Weakness
    T1574.011: Services Registry Permissions Weakness

7. Defense Evasion

T1027: Obfuscated Files or Information
    T1027.003: Steganography
T1014: Rootkit
T1036: Masquerading
    T1036.005: Match Legitimate Name or Location
T1055: Process Injection
T1112: Modify Registry
T1134: Access Token Manipulation
T1218: Signed Binary Proxy Execution
    T1218.001: Compiled HTML File
T1542: Pre-OS Boot
    T1542.003: Bootkit
    T1542.004: Install Root Certificate
T1548: Abuse Elevation Control Mechanism
T1553: Subvert Trust Controls
T1562: Impair Defenses
    T1562.001: Disable or Modify Tools
T1574: Hijack Execution Flow
    T1574.010: Services File Permissions Weakness
    T1574.011: Services Registry Permissions Weakness

8. Credential Access

T1005: Software Deployment Tools
T1080: Taint Shared Content

9. Collection

T1005: Data from Local System
T1039: Data from Network Shared Drive
T1115: Clipboard Data
T1123: Audio Capture
T1125: Video Capture

10. Command and Control

n/a

11. Exfiltration

T1020: Automated Exfiltration
    T1020.001: Traffic Duplication

12. Impact

T1498: Network Denial of Service
    T1498.001: Direct Network Flood

Lapsus$ MITRE ATT&CK Map

1. Reconnaissance

n/a

2. Resource Development

n/a

3. Initial Access

T1078: Valid Accounts
T1133: External Remote Services
T1190: Exploit Public-Facing Application
T1199: Trusted Relationship

4. Execution

T1059: Command and Scripting Interpreter
    T1059.001: PowerShell
    T1059.003: Windows Command Shell
    T1059.004: Unix Shell
T1072: Software Deployment Tools

5. Privilege Escalation

T1068: Exploitation for Privilege Escalation
T1078: Valid Accounts
    T1078.002: Domain Accounts

6. Persistence

T1021: Services
    T1021.001: Remote Desktop Protocol
T1078: Valid Accounts
    T1078.002: Domain Accounts
    T1078.003: Local Accounts
    T1078.004: Cloud Accounts
T1114: Email Collection
    T1114.003: Email Forwarding Rule
T1133: External Remote Services

7. Defense Evasion

T1027: Obfuscated Files or Information
    T1027.002: Software Packing
T1078: Valid Accounts
    T1078.002: Domain Accounts
    T1078.003: Local Accounts
    T1078.004: Cloud Accounts
T1553: Subvert Trust Controls
    T1553.002: Code Signing
T1562: Impair Defenses
    T1562.001: Disable or Modify Tools

8. Credential Access

T1003: OS Credential Dumping
    T1003.001: LSASS Memory
T1111: Two-Factor Authentication Interception
T1212: Exploitation for Credential Access
T1528: Steal Application Access Token
T1552: Unsecured Credentials
    T1552.001: Credentials in Files
    T1552.004: Private Keys
T1555: Credentials from Password Stores
    T1555.005: Password Managers

9. Discovery

T1016: System Network Configuration Discovery
    T1016.001: Internet Connection Discovery
T1069: Groups Discovery
    T1069.002: Domain Groups
T1082: System Information Discovery
T1482: Domain Trust Discovery

10. Lateral Movement

T1021: Services
    T1021.001: Remote Desktop Protocol
T1534: Internal Spearphishing
T1078: Valid Accounts
    T1078.002: Domain Accounts

11. Collection

T1039: Data from Network Shared Drive
T1114: Email Collection
    T1114.003: Email Forwarding Rule
T1213: Data from Information Repositories
    T1213.002: Sharepoint
    T1213.003: Code Repositories

12. Exfiltration

T114: Email Collection
    T1114.003: Email Forwarding Rule
T1537: Transfer Data to Cloud Account
T1567: Exfiltration Over Web Service

13. Impact

T1485: Data Destruction
T1529: System Shutdown/Reboot

Defense Directory   Threat Actors   Tactical Index

References and Sources

In addition to all of the analysts, reporters and organizations listed here, we offer special thanks to the researchers and internal experts at Cyber Security Works and Ivanti, who provided access to industry insights and proprietary information that helped make this Tool Kit possible.

NIST, "Advanced Persistent Threat."

"2022 Global Threat Report." Crowdstrike.

"Alert (AA22-047A): Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology." Cybersecurity & Infrastructure Security Agency (CISA).

"APT29." MITRE ATT&CK.

"Cisco Data Breach Attributed to Lapsus$ Ransomware Group." Dark Reading.

"Cisco Event Response: Corporate Network Security Incident." Cisco Security.

"CISCO Talos shares insights related to recent cyber attack on Cisco." Cisco Talos.

"DEV-0537 criminal actor targeting organizations for data exfiltration and destruction." Microsoft Security.

"Encevo Cyberattack." Encevo.

"Experts Call the Conti Ransomware Gang Who Broke BI Dangerous Hackers." CNN Indonesia.

"General Security Advisory: Understanding and preparing for cyber threats relating to tensions between Russia and Ukraine." National Cyber Security Centre (NCSC).

"Globant official update." Globant.

"Hacker attack on the province of Carinthia: "Black Cat" wants five million dollars in Bitcoin." DerStandard.

"Incident and Agency Updates." Fremont County Colorado.

"Lapsus$: An In-Depth Look at Data Extortion Group." Avertium.

"MITRE Mapping of CISA KEVs and its Challenges." Cyber Security Works.

"Moncler Press Release - Update on Malware Attack." Moncler Group.

"Nordex Group impacted by cyber security incident." The Nordex Group.

"RE: NOTICE OF DATA BREACH." Meyer Corporation.

"RESPONSE TO LATEST MEDIA REPORTS ABOUT 27 NOVEMBER CYBER SECURITY INCIDENT." CS Energy.

"Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability." Cyber & Infrastructure Security Agency (CISA).

"Russia-Nexus UAC-0113 Emulating Telecommunication Providers in Ukraine." Insikt Group: Recorded Future.

"Security update." Uber Newsroom.

"STATEMENT ABOUT CYBERSECURITY INCIDENT: DECEMBER 26, 2021." Shutterfly, Inc.

"Statement from Oiltanking GmbH Group and Mabanaft GmbH & Co. KG Group." Mabanaft Communications.

"Threat Report: T3 2021." ESET Security Research.

"Ubisoft Cyber Security Incident Update." Ubisoft.

"Update on cyber security incident." The Nordex Group.

Abrams, Lawrence. "Lapsus$ hackers leak 37GB of Microsoft's alleged source code." Bleeping Computer.

Abrams, Lawrence. "Shutterfly discloses data breach after Conti ransomware attack." Bleeping Computer.

Amitai Cohen via @AmitaiCo.

Australian Cyber Security Centre (ACSC). "2021-010: ACSC Ransomware Profile - Conti."

Batra, Anirudh. "Detailed Analysis of LAPSUS$ Cybercriminal Group that has Compromised Nvidia, Microsoft, Okta, and Globant." CloudSEK.

Bill Demirkapi via @BillDemirkapi.

Bradbury, David. "Updated Okta Statement on LAPSUS$." Okta.

Brett Callow via @BrettCallow.

Brown, David; Matthews, Michael; Smallridge, Rob. "LAPSUS$: Recent techniques, tactics and procedures." nncgroup.

Burgess, Matt. "The Workaday Life of the World's Most Dangerous Ransomware Gang." Wired.

Cimpanu, Catalin. "Disgruntled ransomware affiliate leaks the Conti gang's technical manuals." The Record.

Clark, Mitchell. "Nvidia says its 'proprietary information' is being leaked by hackers." The Verge.

conti leads via @ContiLeaks.

CÓRDOBA, Javier; Sherman, Christopher. "Cyber attack causes chaos in Costa Rica government systems." AP News.

Culafi, Alexander. "AdvIntel: Conti rebranding as several new ransomware groups." SearchSecurity.

Cyberpedia. "What is the MITRE ATT&CK Framework?" Cortex.

DarkFeed via @ido_cohen2.

DarkTracer : DarkWeb Criminal Intelligence via @darktracer_int.

Davis, Griffin. "'GTA 6' Leaker Arrested! Authorities Claim Teenager is Linked to Lapsus$ Hacking Group." Tech Times.

Digital Security Unit. "Special Report: Ukraine - An overview of Russia's cyberattack activity in Ukraine." Microsoft.

DISSENT. "AlphaV claims attack on Florida International University (updated)." DataBreaches.net.

Fadilpašić , Sead. "Conti ransomware group officially shuts down - but probably not for long." techradar.pro.

Fardkhmanesh, Megan. "The Real Impact of the Grand Theft Auto and Diablo Leaks." Wired.

Fox, Barbara. "Fremont County government services closed due to a cyber security breach." KRDO News.

Ganti, Anil. "Samsung says your personal info wasn't leaked in its recent data hack." SamMobile.

Greenberg, Andy (2019) Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers.

Greenberg, Andy. "Destructive Hacks Against Ukraine Echo Its Last Cyberwar." Wired.

Greig, Jonathan. "BlackCat ransomware group claims attack on Florida International University." The Record.

Greig, Jonathan. "Louisiana authorities investigating ransomware attack on city of Alexandria." The Record.

Greig, Jonathan. "North Carolina A&T hit with ransomware after ALPHV attack." The Record.

Gupta, Surojoy. "All About Conti." Cyber Security Works.

Gurevich, M (1961) The Social Structure of Acquaintanceship Networks, Cambridge, MA: MIT Press

Harbison, Mike; Renals, Peter. "Russian APT29 Hackers Use Online Storage Services, DropBox and Google Drive." Unit 42, Palo Alto Networks.

Hill, Michael. "Cisco admits hack on IT network, links attacker to LAPSUS$ threat group." CSO.

Jenkins, Luke; Hawley, Sarah; Najafi, Parnian; Bienstock, Doug. "Suspected Russian Activity Targeting Government and Business Entities Around the Globe." Mandiant.

Kabelka, Laura. "Austria's Carinthia halts passport issuance over ransomware attack." Euractiv.

Kan, Michael. "Nvidia Confirms Company Data Was Stolen in Hack." PC Mag.

Koczwara, Michael. "LAPSUS$ TTPs."

Lakshmanan, Ravie. "Uber Blames LAPSUS$ Hacking Group for Recent Security Breach." The Hacker News.

Lakshmanan, Ravie. "Uber Claims No Sensitive Data Exposed in Latest Breach... But There's More to This." The Hacker News.

Lyngaas, Sean. "'I can fight with a keyboard': How one Ukrainian IT specialist exposed a notorious Russian ransomware gang." CNN.

Mari, Angelica. "Brazilian Ministry of Health suffers cyberattack and COVID-19 vaccination data vanishes." ZDNet.

Meta / Facebook, "Three and a half degrees of separation."

Minggeng, Liu. "Exclusive / Delta was hacked and extorted 410 million yuan, estimated about 13,500 computers were encrypted." CTWant News.

Newman, Lily Hay. "The Dire Warnings in the Lapsus$ Hacker Joyride." Wired.

Panettieri, Joe. "Lapsus$ Cyberattack vs Okta, Sitel: Up to 366 Okta Customers Impacted." MSSP Alert.

Pearson, James. "UPDATE 4-Shell re-routes oil supplies after cyberattack on German firm." Reuters.

Peters, Jay. "Ubisoft says it experienced a 'cyber security incident', and the purported Nvidia hackers are taking credit." The Verge.

Pink, Bidara. "Last month Bank Indonesia (BI) was hit by a cyber attack, but it has been resolved." Kontan Indonesia.

Polityuk, Pavel. "EXCLUSIVE Ukraine suspects group linked to Belarus intelligence over cyberattack." Reuters.

Ransomware Index Update: Q2-Q3 2022. Cyber Security Works, Ivanti.

Ravindran, Priya. "All about BlackCat (ALPHV)." Cyber Security Works.

Rewards for Justice via @RFJ_USA.

Rockstar Games via @RockstarGames.

Scullion, Chris. "Bandai Namco confirms it's been hacked and says it's investigating damage." VGC News.

Sharma, Ax. "KP Snacks giant hit by Conti ransomware, deliveries disrupted."

Soloman, Howard. "Canadian military provider suffered ransom attack, says news report."

Taipei, Peng Yuwen. "Delta's servers were hacked, and some system recovery operations are estimated to have no major impact." Yahoo News: Taiwan.

Temple-Raston, Dina. "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack." NPR.

The Reliants Project, "Six Degrees of Kevin Bacon."

Tidy, Joe. "Lapsus$: Oxford teen accused of being multi-millionaire cyber-criminal." BBC News.

Todd MicKinnon via @toddmckinnon.

Uchill, Joe. "Globant confirms falling victim to Lapsus$ extortion group." SC Magazine.

Wadhwani, Sumeet. "Former Conti Members Are Now BlackBasta, BlackByte and Karakurt Members." spiceworks.

Wadhwani, Sumeet. "Ransomware Group Lapsus$ Cries Foul After NVIDIA Allegedly Does a Tit-for-Tat." spiceworks.

Werkmeister, Luke. "Ripple effects of ransomware attack against Suffolk County continue more than a week later." The Suffolk Times.

Wolfram, John; Hawley, Sarah; McLellan, Tyler; Simonian, Nick; Veilby, Anders. "Trello From the Other Side: Tracking APT29 Phishing Campaigns." Mandiant.

Zetter, Kim (2015) Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.

2023
Cyberstrategy Tool Kit
for Internal Buy-In

How to Win Budget and Influence Stakeholders
by Explaining Why Your Cybersecurity Strategy
Matters to Non-InfoSec Outsiders

in collaboration with

CSW Cyber
SecurityWorks

ivanti