HONEYWELL 2025 CYBER THREAT REPORT

Insights and Actions to Manage
Cyber-Physical Threat Convergence

June 2025

Honeywell

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Cybersecurity incidents in the past two quarters have impacted operational technology (OT) environments, from transportation sector disruptions to water critical infrastructure attacks. Companies faced increasing cybersecurity and non-compliance risks, as the data in this latest report details. Whether ransomware, worm, USB-carried Trojan virus, or a sentiment-charged attack, the risks are prevalent and require action. New SEC regulations to report cybersecurity incidents only add to the pressure to monitor and defend quickly. Especially for companies with legacy infrastructure, as this report reveals, both historical and new threats need attention.

The two primary challenges are not new: budget constraints and a complex threat landscape. Yet, it's a critical time for the industrial OT cybersecurity domain to leverage cyber-physical and AI-driven methods as threats evolve. Companies are balancing innovation with economic pressures and navigating geopolitical tension by assessing their environments and calibrating their people, process and technology approaches with the latest risk information. Recent outages across global communications providers and varied sector attacks only underscore that no matter the size or scale of your organization, it is always time to better protect your industrial environment.

THREAT REPORT UPDATES

The Honeywell 2025 Cyber Threat Report aims to capture key takeaways and actions at regular intervals. We hope this expert insight supports not only Honeywell's global customer base, but also our collective cybersecurity community. **Only through collaboration and information-sharing can we manage cyber security risks effectively.**

The report delivers data, insights and context to help you better understand and prepare for potential threats.

- **Data:** Includes extensive global data from additional technical solutions embedded across Honeywell customer sites globally to inform a regionally dispersed community.
- **Insights:** Features technical and business findings that are relevant for varied roles across organizations to support researchers, practitioners, policy makers, leadership and more.
- **Context:** Summarizes timely events including new regulations, regional risk findings and summaries of industrial attack campaigns to add context to Honeywell data and insights.

REPORT SOURCE DATA AND METHODOLOGY

This report uses intelligence data primarily derived from Honeywell Cybersecurity solutions from October 1, 2024 to March 31, 2025, unless otherwise displayed or communicated. The solutions analyzed 253.2 billion logs, scanned 79.2 million files and triaged 4,600 events.

KEY FINDINGS

CHANGES IN TYPES OF THREATS

- Honeywell documented a 46% increase in ransomware extortion incidents during the report interval compared to the previous reporting period, with CL0P ransomware group emerging as a dominant actor, surpassing others in activity.
- In the first quarter of 2025, an additional 2,472 reported ransomware victims were documented – on top of the 6,130 identified in 2024.
- Increased prevalence of W32.Worm.Ramnit, typically a banking sector Trojan, deployed to steal industrial account credentials – a 3,000% increase – in the fourth quarter of 2024 compared to when it was last documented in the second quarter of 2024.
- 55% (30 of 55 incidents) of self-reported cybersecurity incidents by companies on SEC Form 8-Ks (under items 1.05, 8.01 and 7.01) in 2024 were reported as direct attacks on a company's operational technology.[1]

46%
INCREASE
RANSOMWARE EXTORTION

2,472
ADDITIONAL
REPORTED RANSOMWARE VICTIMS

CHANGES IN REGIONAL RISK

- The European Union Agency for Cybersecurity's (ENISA) inaugural report highlighted a substantial threat level within the EU[2]. The report emphasized the necessity for enhanced policy implementation, improved cyber crisis management, fortified supply chains and the development of cybersecurity skills to address identified shortcomings.

CHANGES IN HOW SECTORS ARE TARGETED

- Attacks targeting agriculture and food production increased in an exponential pattern.
- Government entities have identified an increase in potential threats for public services:
  - » In the United States, the Environmental Protection Agency (EPA) reported that the drinking water supply for approximately 193 million people is vulnerable to cyberattacks creating a potential for significant disruptions to public health and safety.[3]

Example Incident: In 2024, a large U.S. water and wastewater utility company servicing 14 states was breached, impacting service disruption to several key systems.[4]

- » The Transportation Security Administration (TSA) proposed new cybersecurity regulations for pipelines and railroads, mandating incident reporting within 24 hours and annual cybersecurity evaluations.

Example Incident: A transit system in Pittsburgh, Penn., (USA) was impacted by a ransomware attack causing issues with payment processing for usage of the system.[5]

Example Incident: A Japanese airline experienced a distributed denial-of-service attack that required system shutdowns that delayed more than 40 flights and impacted baggage handling, ticket purchases and more.[6]

THE RISK
LANDSCAPE DYNAMICS

The risk landscape remains dynamic even with continuous efforts to mitigate the impacts breaches and protect ever-interconnected global assets. During the report interval, some companies doubled down on best practices that would be considered baseline, such as immutable data back-ups and regularly scheduled vulnerability assessments. In some cases, these practices prevented significant attack damage. Importantly, it is never too late to start implementing measures. Companies and organizations can always – and regularly do – increase security capabilities relative to their own industrial cybersecurity maturity starting point.

RANSOMWARE, TROJANS
AND USB RISKS

Industrial organizations experienced a notable escalation in threats, particularly from ransomware attacks targeting operational environments during the report interval. Despite the absence of new ransomware variants specifically designed for industrial control systems, existing adversaries continued to disrupt operations across critical sectors. Manufacturing plants, water treatment facilities, and energy providers faced forced production halts, manual failovers, and supply chain interruptions due to ransomware-induced shutdowns.

Similarly, well-known risks such as Trojans not only continued to be present but also in select cases were notably prevalent across the analyzed industrial control system data. USBs continue to carry various types of worm families with a new one identified.

High-profile breaches underscore vulnerabilities within both public and private sectors and should prompt a renewed focus on enhancing cybersecurity protocols and incident response strategies.

THREAT
TYPES

- **User Management and Access Control Attackers**: continue to exploit loopholes in policy administration by looking for high-privilege users, allowed applications and other legitimate-appearing actions to maliciously enter OT networks
- **Ransomware Attackers**: continue to exploit organizations for financial gain using phishing, social engineering and other methods to deploy ransomware.
- **Security Systems Attackers**: continue to target mechanisms and systems that are part of a company's security infrastructure including patch distribution processes and security update packages.

OPPORTUNITIES AND RECOMMENDATIONS

1. **Develop or review policies and procedures:** Create industrial cybersecurity policies, procedures, training and educational materials for your organization. If they already exist, set intervals to review, such as every 15th of the month or during operational quarterly meetings. Policies and standard operating procedures (SOPs) can streamline threat identification, detection and response to threats in an industrial control network and reduce delays and damage when an attack occurs.

   These steps also prepare cross-functional teams and help build relationships that will be crucial when an attack occurs.

2. **Train employees:** Educate employees on how to identify and avoid phishing attempts and how to maintain good cyber hygiene practices.

3. **Protect against USB threats:** Scan removable media like UBSs with products from approved vendors to help reduce the threat vector of malware and ransomware from entering the environment.

4. **Use multi-factor authentication:** Enable strong passwords and multi-factor authentication (MFA). Adopt password vaults and push to identify access.

5. **Segment networks:** Isolate systems to limit the spread of attacks.Practise principles of least privilege by granting users, devices and applications only the access they need to perform their tasks to help lower the potential for a breach.

6. **Deploy Zero Trust Architecture (ZTA):** Assume no implicit trust between systems. Verify every user, device and workload accessing your OT environment. Implement least privilege access, micro segmentation and strong identity controls. Once these recommendations are standard practice, then trusting a data view only for advanced process control, predictive maintenance, risk analysis, operational excellence, advanced threat monitoring becomes easier.

7. **Update software:** Conduct regular system updates to fix vulnerabilities and integrate with a patch management and update delivery solution. When operationally feasible, this can identify software update issues and can impact the integrity of the software operating environment.

8. **Monitor and audit:** Monitor and assess security measures using readily available tools to stay ahead of threats, by visualizing network communications and taking actions on erroneous operations and communications.

OPPORTUNITIES AND RECOMMENDATIONS

9. **Encrypt data:** Protect sensitive data, both at rest and in transit.

10. **Back up and recover:** Protect data integrity and operational continuity by implementing secure, air-gapped or immutable backups of critical systems and configurations. Enable point-in-time recovery and regularly test it in case of ransomware or sabotage.

11. **Conduct vulnerability assessments:** Execute vulnerability assessments.

12. **Label critical assets:** Append additional context to asset records such as which systems are critical and need to be prioritized.

13. **Use industry approved standards:** Comply with these frameworks to cover the minimum requirements for security-relevant aspects for a given industry and secure critical assets:
    - » NIST 800-82
    - » IEC 62443
    - » NERC CIP

14. **Create a secure IT/OT Integration:** Use cloud services specifically designed to securely bridge IT and OT. Isolate critical OT systems from direct cloud exposure and use secure data brokers or gateways for telemetry. Telemetry and Control do not need to be performed in the same signal or even with the same equipment. Isolating control away from telemetry provides method to leverage the wave of new offerings from various AI providers while protecting critical systems.

15. **Leverage cloud-native security controls:** Take advantage of cloud provider tools that include native security controls:
    - » Identity and access management
    - » Logging and moniroting (e.g., AWS CloudTrail, Azure Defender, GCP Security Command Center)
    - » VPC peering
    - » Service Level Encryption
    - » Vulnerability management tied to CI/CD pipelines.

HONEYWELL PRODUCT INTELLIGENCE

This report uses intelligence data from the following Honeywell Cybersecurity solutions from October 1, 2024 to March 31, 2025, unless otherwise displayed or communicated.

- **Honeywell Advanced Monitoring and Incident Response (AMIR)**: A Honeywell Managed Security Service (MSS) that uses Honeywell's cyber professionals to assist customers in actively monitoring in-scope networks for signs of a cyberattack to help improve proactive incident response in complex environments.

- **Honeywell Secure Media Exchange (SMX)**: A cyber-physical solution that provides enforceable enterprise USB and removable media protection, that uses Honeywell Cyber Threat Intelligence with enriched data from Google Threat Intelligence (GTI) for deep data inspection. SMX is deployed through a notebook-like digital device or a kiosk-like physical set-up, on premises at industrial sites. Personnel are required to scan their device before it is brought into the facility for use.

- **Honeywell Cyber Insights**: A cyber-physical solution combining on-premise OT data insights delivered through a threat intelligence feed, together with site management software-as-a-service. It provides near real-time data on identified threats, anomalous behavior and vulnerabilities to help organizations reduce and manage an individual site's cybersecurity risks.

- **Honeywell Cyber Watch**: A software-led solution designed to provide users with an enterprise-wide (multi-site) view of their OT cybersecurity posture along with a compliance dashboard for global frameworks and internal policy management. It aggregates data from Cyber Insights installations at each site, allowing users to monitor their cybersecurity posture across all locations.

- **Honeywell Professional Cybersecurity Services**: A managed service leveraging Honeywell OT cybersecurity professionals who work closely with global customers and use their first-hand knowledge of industrial control systems and potential risks to those systems. They can deliver more than 30 services such as conducting risk assessments, implementing defenses and helping plan more effective incident response.

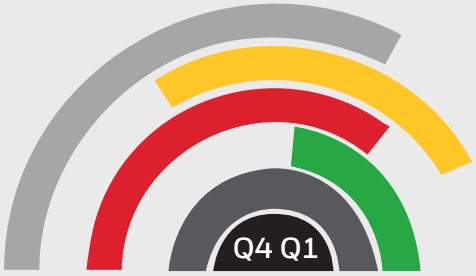
HONEYWELL AMIR FINDINGS

POLICY ENFORCEMENT AND CONSISTENT HARDENING CAN IMPROVE RISK MANAGEMENT

The Honeywell Advanced Monitoring and Incident Response (AMIR) service, as part of Honeywell Managed Security Services (MSS), provided the following data for this risk report interval.

89.9 Billion

There were 89.9 Billion Logs Analyzed over Q4 2024 & Q1 2025 by Honeywell **AMIR**



There were 1,008 Incidents that were triaged out of 54,098 Alerts over Q4 2024 and Q1 2025

1,008

107

There were 107 Unique Incidents triaged over Q4 2024 and Q1 2025

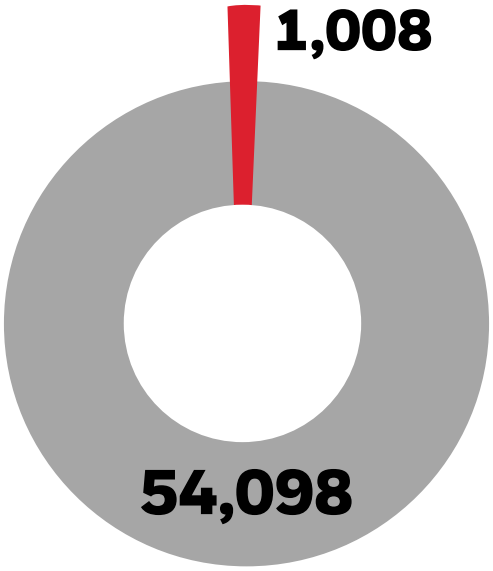


Figure 1 Honeywell AMIR Telemetry

DETECTED 107
UNIQUE INCIDENTS

During the reporting period, Honeywell AMIR triaged 54,098 alerts resulting in 1,008 incidents, and of those, there were 107 unique incidents detected. Let's review the top four types of incidents from those 107 events and discuss recommendations for future remediation.

Top Four Types of Incidents:

1. USB plug and play
2. Account was added to a local security group
3. CB-AppControl enforcement level changed from high to low
4. Member was added to a domain controller's security group

Incident Name	No.
1. USB Plug and Play	84
2. Account Was Added To a Local Security Group	62
3. CB-AppControl Enforcement Level Changed From High To Low	42
4. User Account Created	39

Figure 2 Honeywell AMIR Incidents and number of occurances

1. USB PLUG AND PLAY

Among the incidents identified by Honeywell AMIR, 25% of the top 10 incidents were triggered by USB plug and play. A USB plug-and-play incident can pose a significant cybersecurity risk, especially when an unauthorized or malicious device is connected to a system. For example, an employee might unknowingly insert an infected USB drive into a corporate computer, triggering an automatic execution of malware designed to steal sensitive data or deploy ransomware. In a recent case, a company experienced a security breach when a seemingly harmless promotional USB stick, distributed at a trade show, contained a hidden payload that installed a keylogger on the network. Modern operating systems often auto-detect and interact with USB devices without user intervention, allowing attackers to exploit this feature to execute scripts or alter system settings.

Recommendation: Endpoint security measures are critical. Disable USB ports when not needed, implement device control policies, introduce Secure Media Scanning Kiosks, and educate employees on the dangers of unknown USBs or removeable media devices.

2. ACCOUNT ADDED TO LOCAL SECURITY GROUP

Representing 16% of the Honeywell AMIR recorded top incidents, adding accounts to local security groups can create security risks because it grants elevated access to a system. Adding users to privileged groups like “Administrators” can potentially allow unauthorized users to make critical changes or access to sensitive data if compromised, especially when not managed centrally through a domain environment. This can be particularly concerning if too many accounts are added to these groups, leading to excessive permissions and potential for misuse.

Recommendation: Evaluate what criteria will be used for selecting which accounts constitute privileged and non-privileged groups. Set up mechanisms to enforce. Regularly audit and review account lists to look for changes in privilege or newly added privileged accounts.

3. REVIEWING CIS BENCHMARKS FOR WINDOWS ENTERPRISE DESKTOPS

The Center for Internet Security (CIS) Benchmarks are globally recognized security standards that help organizations defend their IT/OT systems and data from cyberattacks. They are created by a community of cybersecurity experts, compliance and security professionals. They create a checklist of best practices that can be applied multiple to different technologies.

The following are examples from the Microsoft Windows 10 Enterprise Benchmark and identified by the Honeywell AMIR team:

2.2.16 Ensure ‘Deny access to this computer from the network’ to include ‘Guests, Local accounts’

2.2.20 Ensure ‘Deny log on through Remote Desktop Services’ to include ‘Guests, Local accounts’

2.3.10.12 Ensure ‘Network access: Sharing and security model for local accounts’ is set to ‘Classic – local users authenticate as themselves’

18.4.1 Ensure ‘Apply UAC restrictions to local accounts on network logons’ is set to ‘Enabled’

18.10.4.3 Ensure ‘Prevent the use of security questions for local accounts’ is set to ‘Enabled’

Recommendation: Keep track of configuration changes and address configuration drift in programmatic ways as part of a detection-in-depth approach.

3. CB-APPCONTROL ENFORCEMENT LEVEL CHANGED FROM HIGH TO LOW

Enforcement Level is the protection level applied to computers running the Carbon Black App Control Agent, specified on a per-policy basis. Enforcement Levels, which vary in restrictiveness, affect how file actions are controlled for policy settings. File-blocking and other control functions in Carbon Black App Control depend on both the Enforcement Level and on specific policy settings in effect, including policy-specific bans. In Control mode, you choose High (Block Unapproved), Low (Monitor Unapproved), or Medium (Prompt Unapproved) Enforcement Level from a menu. The other modes, None (Visibility) and None (Disabled), automatically designate the Enforcement Level as None.

Essentially, these incidents declare that a customer is moving from a "White List" approach to a "Black List" approach inside their environment. This means instead of only allowing approved files on a "White List" to run, install and launch, now all files are allowed to use all actions unless there are known bad files on a "Black List" which should not be authorized. Moving to a Low Enforcement level allows users to be more productive and take on the personal control of managing security and risk through responsible utilization of file usage.

Recommendation: Adjust enforcement policies and strategies based on your unique environment, particularly domain expertise level, and consider use of application control solutions to track changes. Downgrading from a high to a lower enforcement level is not typically recommended. Instead, take one of the following approaches to facilitate the execution of a file that may be blocked by App Control, especially if the file's hash is previously unknown to the system.

Use **Publisher and Certificate-based approvals**. If the file contains a valid publisher and a trusted certificate, App Control can permit execution based on this combination. Configure **customized rules** such as **execution control** or **file write** for files lacking publisher or certificate information to allow execution in a controlled manner.

4. MEMBER WAS ADDED TO A DOMAIN CONTROLLER'S SECURITY GROUP

Active Directory Users' and Computers' "Security Enabled" groups are simply referred to as Security groups. Active Directory (AD) has two types of groups: Security and Distribution. Security (security enabled) groups can be used for permissions, rights and as distribution lists. Distribution (security disabled) groups are for distribution lists in Exchange and cannot be assigned permissions or rights. Global means the group can be granted access in any trusting domain but may only have members from its own domain. This event is only logged on domain controllers. Every user added to a Domain Controller's Security Group creates one more vector for attackers to leverage.

Recommendation: Conduct identity audits to fully understand the number of assets and resources that members can access or control inside the industrial control environment to help navigate any potential future incidents.

HONEYWELL SMX FINDINGS

MEASURES AGAINST TROJANS AND WORMS REQUIRE CONSTANT UPDATES THROUGH AUTOMATED TOOLS AND SCRIPTS.

Hackers will use any means possible to access an industrial control network and do not distinguish the age of a penetration technique or system vulnerability. This includes worms, Trojans, viruses and malware of any kind, which can often go completely unnoticed if delivered through a removable device like a USB or a removeable media device. Trojans and worms require constant updates through automated tools and scripts to scale defenses to address the level of risk.

Deploying physical controls to assist in policy enforcement can help organizations manage USB threat risk. Honeywell SMX, which is designed to detect risks in USB devices, found several notable incidents during the report interval.

31.4 Million

There were 31.4 million Files Scanned over Q4 2024 & Q1 2025 by Honeywell SMX global installs

There were 1,826 Unique Threats detected over Q4 2024 & Q1 2025

1,826

Between Q4' 23 & Q1'24 and Q4 of 2024 and Q1 of 2025 there have been 5 Million more files scanned in last two Quarters than the previous year.

5M+

4,984

Of the 31.4 million files scanned over Q4 2024 & Q1 2025, 4,984 were blocked or prohibited from running on customers endpoints

Figure 3 Honeywell SMX/GARD Telemetry

DETECTED 1,826 DISTINCT THREATS

During the reporting period, Honeywell SMX scanned 31.4 million files and identified 4,984 threats with 1,826 distinct threats. This included 124 unique threats not seen in previous reporting periods. This indicates that tactics and threats increased during the current reporting period. Forty-two percent of detected threats can be attributed to: Win32.Worm.Ramnit, Trojan.scar/shyape, Trojan.lokibot/stealer, and Win32.Worm.Sohanad.

Let's review these threats and discuss recommendations for future remediation.

100 TOP THREATS & NUMBER OF TIMES IDENTIFIED

Threat Name	No.	Threat Name	No.	Threat Name	No.
Win32.Worm.Ramnit	699	Win32.Downloader.Upatre	27	ByteCode-MSIL.Trojan.Ribaj	16
trojan.scar/shyape	264	trojan.razy/qakbot	27	Win64.Backdoor.CobaltStrike-Beacon	15
trojan.lokibot/stealer	224	ransomware.globeimposter/encoder	27	trojan.zusy/predator	15
trojan.dorkbot/locky	123	Win32.Trojan.Sivis	26	trojan.netwire/weecnaw	15
trojan.scar/doina	91	trojan.netwire/netwiredrc	25	trojan.mansabo	15
trojan.seven/lockfile	88	Win32.Adware.DealPly	24	trojan.adwind/java	15
Win32.Worm.Sohanad	88	trojan.msil/blocker	24	Win32.Worm.Ludbaruma	14
Win32.Hacktool.PwDump	80	Win32.Trojan.CobaltStrike	23	Win32.PUA.DownloadGuide	14
trojan.prometei/variadic	77	Win32.Worm.RontoKbro	22	trojan.scar/cmrab-m6e8rb	14
trojan.loki/lokibot	67	virus.floxif/pioneer	22	trojan.qbot/zusy	14
ransomware.sodinokibi/sodin	66	trojan.zbot/spyeye	21	trojan.netwire/razy	14
trojan.kwampirs/bedep	65	trojan.qbot/qakbot	21	trojan.padodor/shellobject	14
trojan.weecnaw/netwire	64	trojan.qbot/razy	21	trojan.netwire/doina	14
DOS.Malware.EICAR	62	trojan.mansabo/dndy	21	trojan.vtflooder/badur	13
ransomware.sodinokibi/dump	51	trojan.mansabo/botx	21	trojan.zbot/autoit	13
virus.eicar/test	47	trojan.msil/razy	21	trojan.qukart/berbew	13
Win32.Ransomware.GandCrab	44	Win32.Packed.Themida	20	trojan.msil/jalapeno	13
trojan.starter/ramnit	44	trojan.avaddon/zenpak	20	Win32.Worm.Palevo	12
trojan.icedid/inject3	43	trojan.dorkbot/sirfvog	20	Win32.Worm.AutoRun	12
Win32.Trojan.Delf	42	Win32.Keylogger.EliteKeylogger	19	Win32.Virus.Ausiv	12
ByteCode-MSIL.Backdoor.Bladabhindi	41	trojan.msil/banload	19	Win64.Hacktool.PwDump	12
Win32.Ransomware.VirLock	40	miner.dacic/deepscan	19	Win32.Ransomware.TeslaCrypt	12
ransomware.sodinokibi/revil	39	Win32.Virus.Expiro	18	Win32.PUA.FlyStudio	12
trojan.dorkbot/sodinokibi	37	Win32.PUA.InstallMonster	18	Win32.Downloader.Unruy	12
trojan.banbra/barys	35	trojan.upatre/ppatre	18	Win32.Hacktool.Fg-dump	12
trojan.dorkbot/ngrbot	35	trojan.paneidix/marte	18	trojan.zbot/natas	12
trojan.qbot/mikey	34	trojan.cosmu/zombie	18	trojan.zbot/boigy	12
Script-JS.Worm.Cassa	34	Script-JS.Trojan.Miner	18	trojan.java/adwind	12
Win32.Trojan.Generic	32	trojan.icedid	17	Win32.Worm.Conficker	11
Win32.Dropper.GepSys	32	trojan.dorkbot/deepscan	17	Win32.Spyware.Actual-Spy	11
Win32.Exploit.CVE-2010-2568	31	Win32.Trojan.Zpevdo	16	Win32.Keylogger.SpyTector	11
Win32.Worm.Mofksys	28	Win32.Hacktool.Cain	16	trojan.ursnif/razy	11
trojan.padodor/berbew	28	Win32.Hacktool.JohnTheRipper	16		
trojan.dacic/vbclone	28	ransomware.sodinokibi/del-shad	16		

Figure 4 Honeywell SMX/GARD Threat Intel showing top 100 threats and number of times identified

WIN32.WORM.RAMNIT

Thirty-seven percent of files blocked by Honeywell SMX during the report period contained W32.Worm.Ramnit. **This is a 3,000% increase since it was last observed in Q2 2024.** W32.Rmnit is primarily a banking trojan used to steal account credentials; however, given its saturated presence in Honeywell industrial customers' ecosystems, it can likely be assumed it has been repurposed to extract control system credentials.

Recommendation: Monitor IT network Trojans since they may cross over into variants deployed in OT networks. Deploy detection rules to monitor for instances in your organization. See sample rules shared in this report.

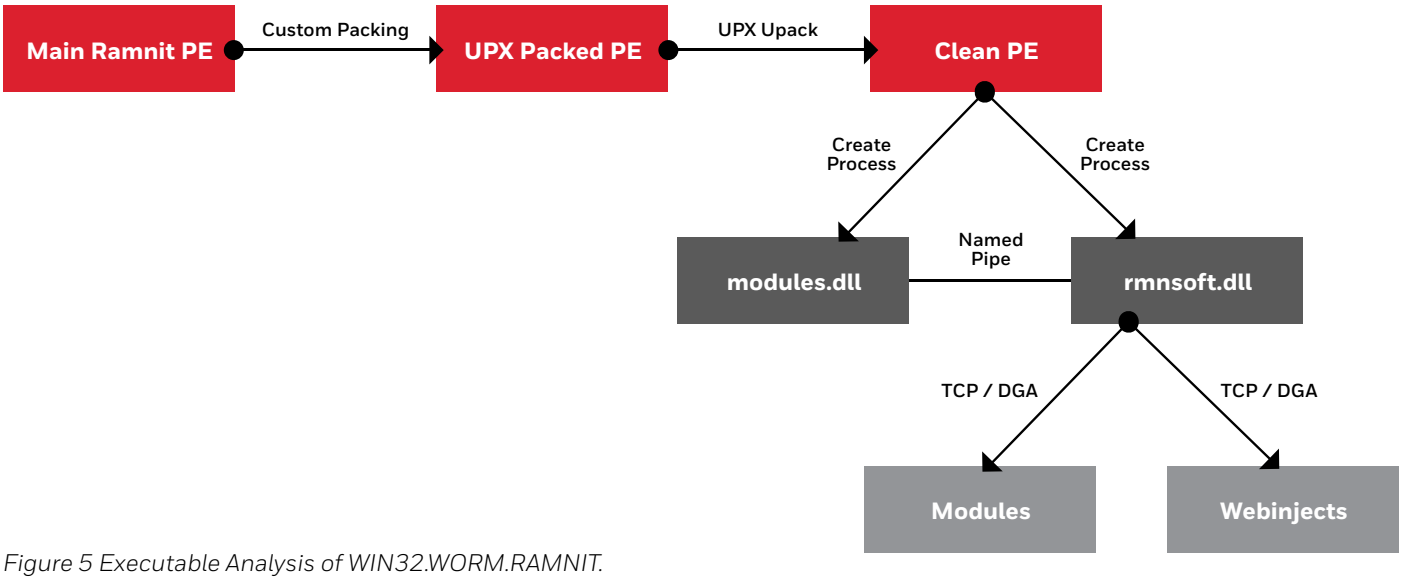


Figure 5 Executable Analysis of WIN32.WORM.RAMNIT. Source: Michal Praszmo'

File Names Detected:

npswf32.dll | ouThvPKt.cpl | trLgkCKs.cpl | CllUKcKo.cpl

ySeAWYQp.cpl | DUukBXpr.cpl | YbffZnwd.cpl

YARA Rule for Detection:

paper.0f2d416ac126f4488398e67a69c59c91.yaml · GitHub

https://malpedia.caad.fkie.fraunhofer.de/yara/win.ramnit

TROJAN.SCAR/SHYAPE

A rise in incidents involving Trojans encapsulated in ransomware appeared during the report interval. Shyape, which is known by many names, had a high hit rate for files blocked from execution at customer sites globally. Although the ability to reverse and wipe this nuisance software is an easy task, if it breached the perimeter and made its way into operational control systems, it could be an arduous event for the security team tasked with performing incident response.

Malware Samples

The table below shows all malware samples that are associated with this particular tag (**max 400**):

Firstseen (UTC)	SHA256 hash	Tags	Signature	Reporter
2012-09-06 06:46:04	9481057b81fcf44fc0667d...	exe Shyape	Shyape	JAMESWT_WT
2012-09-06 06:46:00	2034913d5e026d6202f5...	exe Shyape	Shyape	JAMESWT_WT
2012-09-06 06:45:57	764584f517064ea8c3e3e...	exe Shyape	Shyape	JAMESWT_WT

TROJAN.LOKIBOT/STEALER

LokiBot targets Microsoft Windows-based systems to steal credentials and harvest sensitive information ranging from usernames, passwords and user data from browsers, messaging applications, email, FTP clients and cryptocurrency wallets. It uses a .NET launcher and can download and execute other binaries to harvest data via HTTP. LokiBot is also known as "Purecrypter" and "Mosaicloader" and linked with malware families such as BETABOT, LUMINOSITYLINK and FORMBOOK. It is known to target industries such as chemicals, construction, education, financial services, government, hospitality, manufacturing, pharmaceuticals, telecommunications and transportation, exploiting vulnerabilities such as CVE-2021-40444 and CVE-2022-30190. It attacks using OS credential dumping, keylogging, process injection and masquerading and is often distributed through spear-phishing emails with malicious attachments.

Recommendation: Use the CISA-developed Snort signature to detect network activity associated with LokiBot activity:

```
alert tcp any any -> any $HTTP_PORTS (msg:"Lokibot:HTTP URI POST contains
contains '/*/fre.php' post-infection"; flow:established,to_server ; flowbits:isnotset,.
tagged; content:"/fre.php"; http_uri; fast_pattern:only; urilen:<50,norm; content:"POST";
nocase; http_method; pcre:"/\/(?:alien|loky\d|donep|jemp |lokey|new2|
loki|Charles|sev 7n|dbwork|scroll \/NW|wrk|job|five\ d?|donemy|animation \
dkc|love|Masky|v\d |lifetn|Ben)\/fre\ .php$/iU"; flowbits:set,.tagged
;classtype:http-uri; metadata:service http; metadata:pattern HTTP-P001,)
```

WIN32.WORM.SOHANAD

The report period saw a new worm in devices: Win32.Worm.Sohanad. Sohanad is a family of worms that spread via removable media or network drives. Worms and viruses work to open backdoors on the exploited computer to allow a persistent connection for complete control and future access.

Below is an example of loaded files and altered registered post infection of this worm:

- [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] "Msn Messsenger"="C:\WINDOWS\system32\regsvr.exe"
- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon] "Shell"="Explorer.exe regsvr.exe"
- [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Schedule] "AtTaskMaxHours"=0x00000000
- [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Schedule] "NextAtJobId"=0x00000002
- [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services\Schedule] "AtTaskMaxHours"=0x00000000
- [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services\Schedule] "NextAtJobId"=0x00000002
- [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\WorkgroupCrawler\Shares] "shared"="\New Folder .exe"
- [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings] "GlobalUserOffline"=0x00000000
- [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer] "NofolderOptions"=0x00000000
- [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System] "DisableRegistryTools"=0x00000001
- [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System] "DisableTaskMgr"=0x00000000

Recommendation: Deploy detection rules to monitor for instances in your organization and use physical controls to manage USBs brought on site. See sample rules shared in this report.

Suricata Rule for Detection:

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET WORM Possible Worm Sohanad.Z or Other Infection Request for setting.nql"; flow:established,to_server; content:"/setting.nql"; nocase; http_uri; reference:url,www.threatexpert.com/report.aspx?md5=a70aad8f27957702febfa162556dc5b5; classtype:trojan-activity; sid:2012201; rev:3;)

WIN32.EXPLOIT.CVE-2010-2568

Win32.Exploit.CVE-2010-2568 identifies malicious shortcut LNK files designed to exploit the known CVE-2010-2568 vulnerability in the shell program of various versions of Microsoft Windows (XP SP3, Server 2003 SP2, Vista SP1 and SP2, Server 2008 SP2 and R2, and Windows 7) by allowing remote code execution simply by browsing a folder containing a malicious .LMK file. The CVE-2010-2568 vulnerability was notably used by Stuxnet to gain access to target systems and has been used by other malware families.

Please reference this Microsoft Security Bulletin MS10-046 to learn more on how to protect your systems.

Recommendation: Prioritize patch management. First: apply critical patches such as Microsoft Security Patch MS10-046.

Recommendation (con'd.): Use robust alternative controls for systems that can't be promptly patched, including:

- Employ strong network segmentation using firewalls and VLANs to isolate vulnerable assets and limit communication.
- Disable autorun and autoplay features and implement media exchange barriers to prevent malware execution from removable media.
- Enforce strict policies and technical controls for removable media usage including mandatory scanning and port disabling.
- Restrict access to network shares, particularly writable shares.
- Use application allowlisting when feasible and cautiously deploy vendor-approved endpoint security solutions to enable compatibility and up-to-date signatures specific to identified threats.
- Consider Intrusion Prevention Systems with virtual patching capabilities to enhance security.
- Implement proactive detection and monitoring to rapidly identify anomalies or malicious connections with routine analysis of relevant systems and security logs.
- Harden system regularly by disabling unnecessary services and consistently enforcing the principle of least privilege for all user and service accounts.
- Develop and routine test an OT-specific incident response plan that outlines procedures for the safe isolation of systems, malware containment and operational recovery with minimal impact on physical processes.

HONEYWELL COMMUNITY INTELLIGENCE

The following section draws from OSINT data as well as multiple cross-industry sources to provide additional context to the product-driven data above.

RANSOMWARE GROUPS

Ransomware groups are organized cybercriminal entities that deploy malicious software designed to encrypt victim's data and demand a ransom for its release. These groups often operate like businesses with specialized roles including developers who create the malware, operators who deploy the attacks, and negotiators who handle ransom demands. They target a wide range of victims from individual users to large corporations and government entities. Ransomware tactics continue to evolve and can leverage various attack vectors such as phishing emails, smishing attacks, exploit kits and remote access vulnerabilities to infiltrate systems. These groups often pose a significant challenge to cybersecurity professionals with their sophistication and ability to obscure financial transactions and communications. A robust, multi-layered defense strategy is necessary to protect against ransomware attacks.

IDENTIFIED 1,929 RANSOMWARE ATTACKS

During the reporting period, 1,929 ransomware attacks were publicly documented with 71% of attacks occurring in eight verticals with manufacturing, construction, healthcare and technology companies seeing the most impact. Ransomware attacks tend to be more opportunistic, typically creating a normal distribution of attacks across different industries. That said, attacks on agriculture and food production organizations are exponentially increasing.

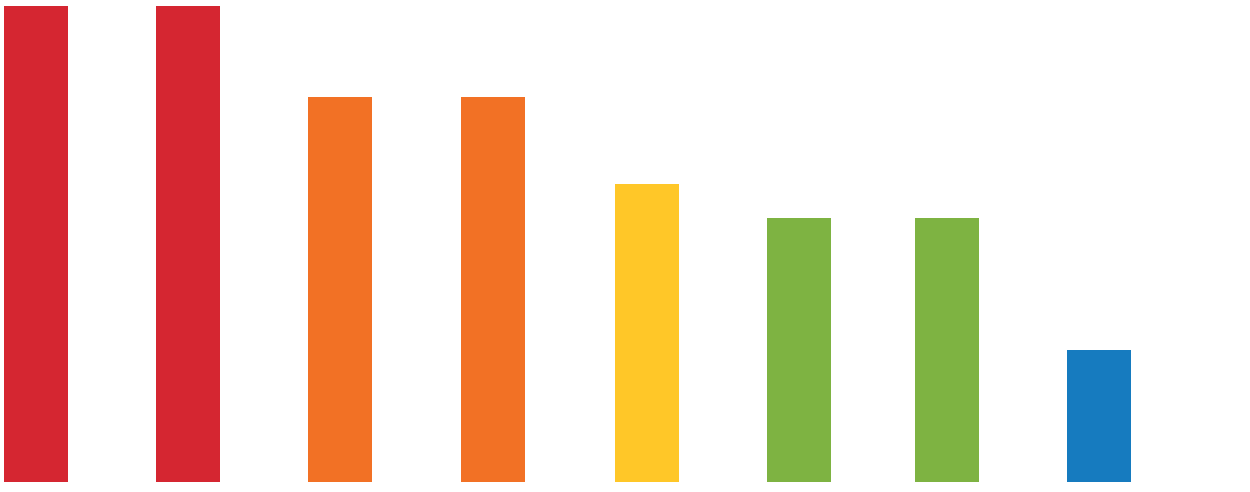
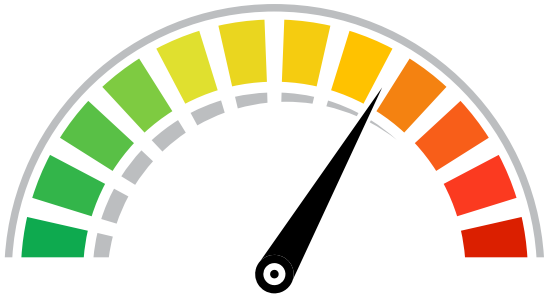


Figure 6 Q4 documented victim industries
Source: Ransomware.live

TOTAL TRACKABLE RANSOM PAID

Ransomwhere is an open, crowdsourced ransomware payment tracker.

As of October 2024, over $1 billion in ransomware was paid out by victimized companies.



$1,018,573,922

STAY VIGILANT OF RANSOMWARE GROUPS

Group name	Active	Last Update	Victims Detected
lockbit3	●	2024-11-12 14:45	1969
lockbit2	●	n/a	1006
alphv	●	2024-03-09 15:07	732
play	●	2024-11-12 14:55	686
clop	●	2024-11-12 16:02	540
bianlian	●	2024-11-12 15:57	505
ransomhub	●	2024-11-12 14:57	499
blackbasta	●	2024-11-12 15:58	482
8base	●	2024-11-12 15:51	415
conti	●	2024-03-30 16:43	351
dispossessor	●	2024-08-12 13:20	344

Figure 7 Ransomware Groups Driving Attacks in 2024
Source: Ransomware.live

CL0P

CL0P ransomware is operated by the cybercriminal group TA505. The Cyber Canadian Centre assesses that TA505 is most likely a financially motivated, Russian-speaking, ransomware-as-a-service (RaaS) cybercrime group likely based in a Commonwealth of Independent States (CIS) country. A RaaS cybercrime group maintains the functioning of a particular ransomware variant, sells access to that ransomware variant to individuals or groups of operators (often referred to as "affiliates"), and supports affiliates' deployment of their ransomware in exchange for upfront payment, subscription fees, a cut of profits, or all three.

TA505 has been active since at least 2014. In addition to operating the CL0P RaaS, TA505 also operates as:

- an affiliate or developer of other RaaS operations including LockBit, Hive, Locky Ransomware and REvil;
- an initial access broker, selling access to compromised corporate networks;
- a large botnet operator, specializing in financial fraud and phishing attacks, involving use of the Dridex banking trojan.

CL0P ransomware was first observed internationally in 2019 and is possibly an evolution of CryptFile2, CryptoMix and Work ransomwares.[7]

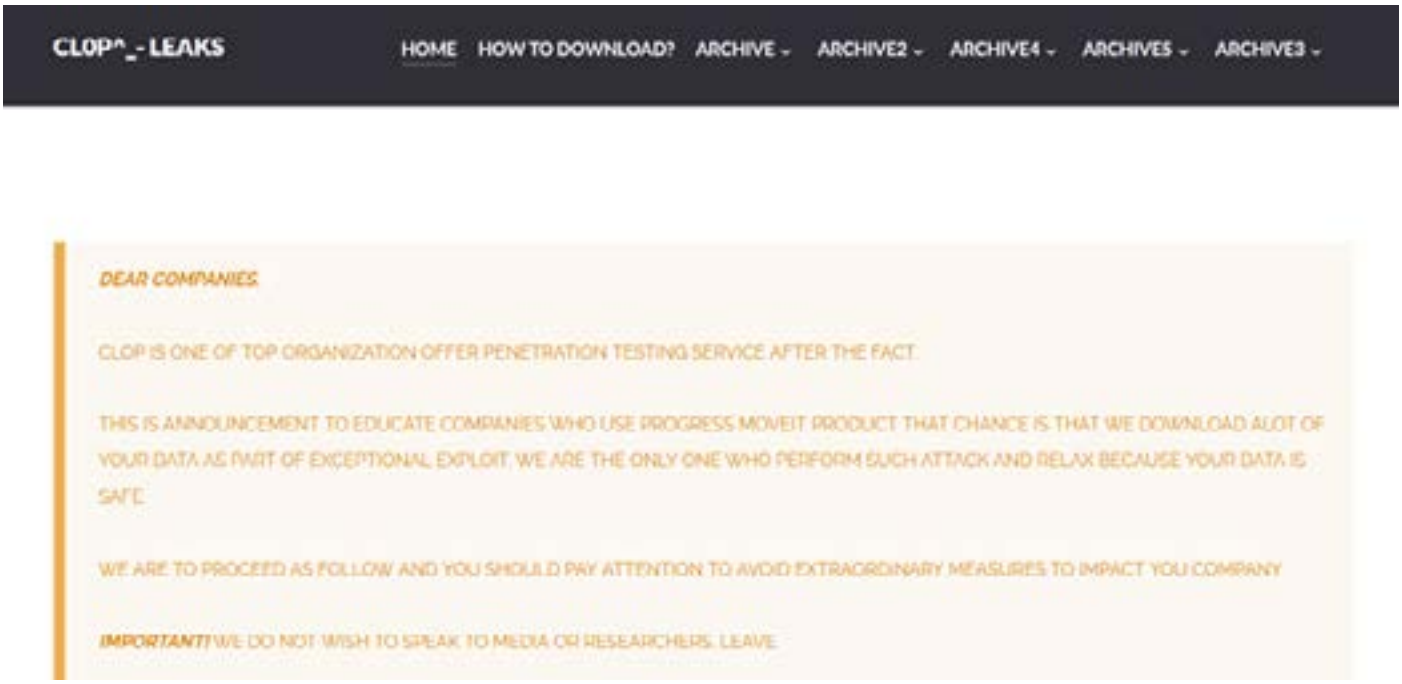


Figure 8 CL0P Leaks Dark Web message from attackers

SAMPLE OF CL0P VICTIMS FOR Q4 2024

There were approximately 73 CL0P documented victims during the report interval with the majority of attacks occurring in December.

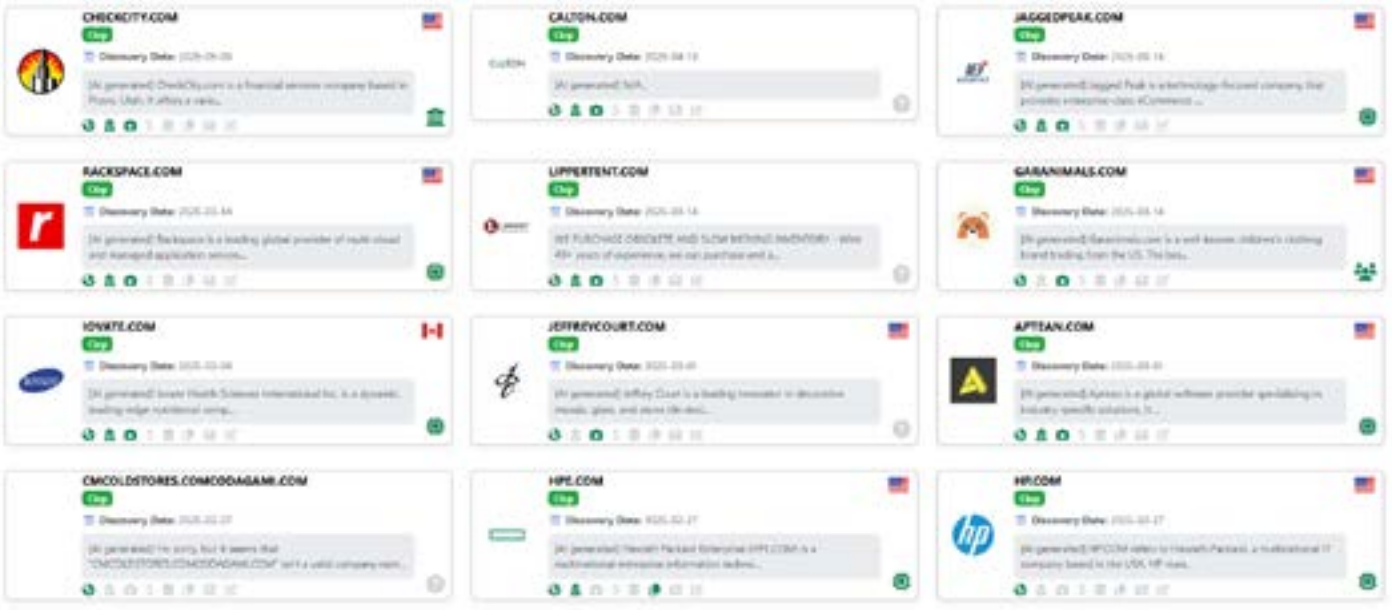


Figure 9 Ransomware.live Victims of Cl()p

TACTICS, TECHNIQUES AND PROCEDURES OF CL0P DURING REPORT INTERVAL

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Phishing: Spearphishing Attachment	Native API	Boot or Logon Autostart Execution	Domain Policy Modification: Group Policy Modification	Masquerading: Invalid Code Signature	File and Directory Discovery	Lateral Tool Transfer	Data from Local System	Application Layer Protocol	Exfiltration Over Web Service	Data Encrypted for Impact
Exploit Public-Facing Application	Command and Scripting Interpreter	Create or Modify System Process: Windows Service	Exploitation for Privilege Escalation	Impair Defenses: Disable or Modify Tools	Remote System Discovery	Remote Services: SMB/Windows Admin Shares				Inhibit System Recovery
Valid Accounts	User Execution		Hijack Execution Flow	Deobfuscate/Decode Files or Information	Process Discovery					
				Indicator Removal on Host: File Deletion	System Information Discovery					
				Process Injection: DLL Injection	Query Registry					
				Indirect Command Execution	Security Software Discovery					
				Indicator Removal on Host: Clear Windows Event Logs						

Figure 10 Tactics, Techniques and Procedures
Souce: randsomeware.live

OBSERVED VULNERABILITIES USED BY CL0P

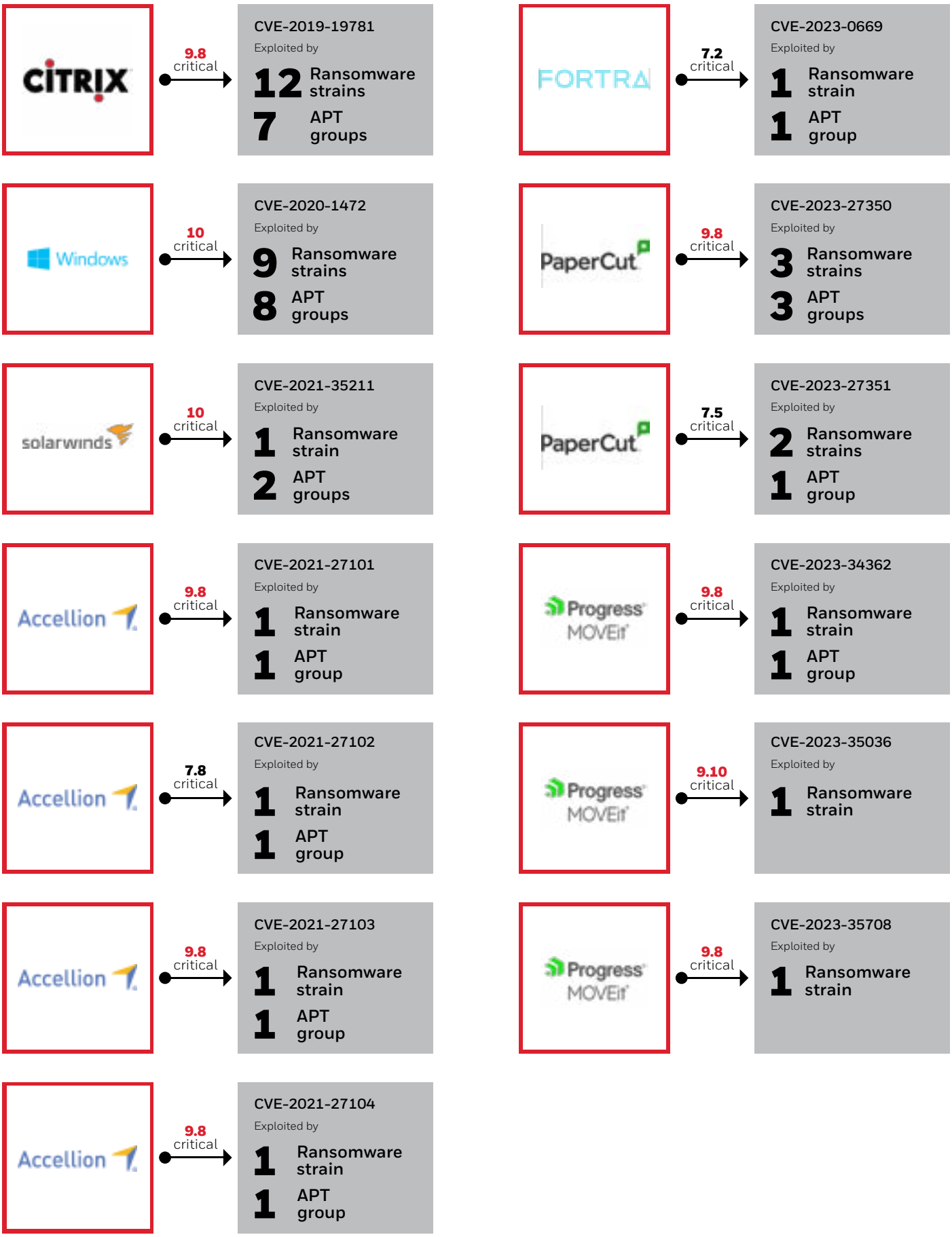


Figure 11 Vulnerabilities Used by CL0P

Below we explore one of the main vulnerabilities that CL0P uses when compromising victims.

CVE-2023-27350

Allows remote attackers to bypass authentication on affected installations of PaperCut NG 22.0.5 (Build 63914). The specific flaw exists within the “SetupCompleted” class and is a result of improper access control. An attacker can use this vulnerability to bypass authentication and execute arbitrary code in the context of SYSTEM.[8]

Details

PaperCut servers vulnerable to CVE-2023-27350 will implement improper access controls in the SetupCompleted Java class, allowing malicious actors to bypass user authentication and access the server as an administrator. After accessing the server, actors can leverage existing PaperCut software features for remote code execution (RCE). There are currently two publicly known proofs of concept for achieving RCE in vulnerable PaperCut software:

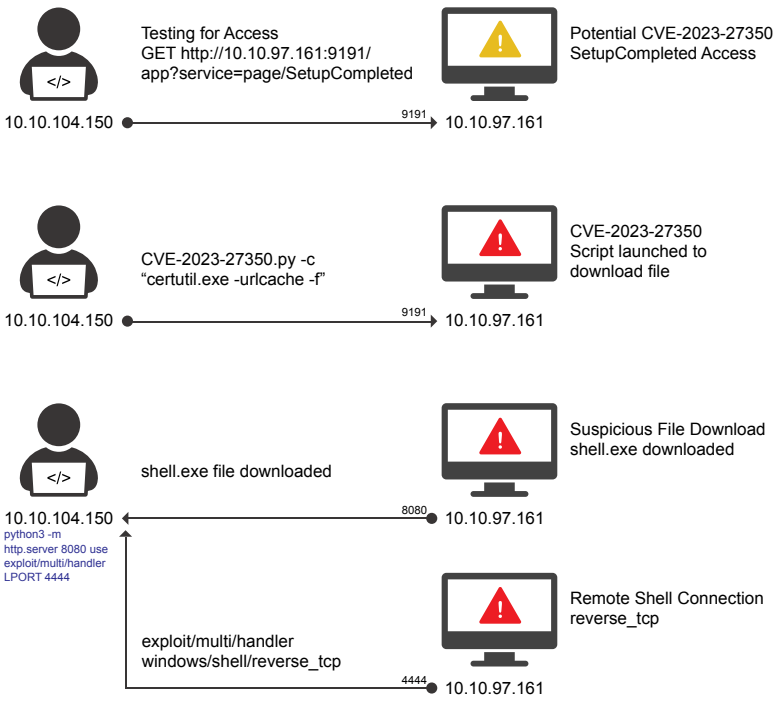
- Using the print scripting interface to execute shell commands
- Using the User/Group Sync interface to execute a living-off-the-land-style attack

Both the FBI and CISA believe bad actors may develop other methods for RCE.

The PaperCut server process pc-app.exe runs with SYSTEM- or root-level privileges. When the software is exploited to execute other processes such as cmd.exe or powershell.exe, child processes and commands can be created with the same privileges. As a result, a wide range of post-exploitation activity is possible following the initial access and compromise.

CISA added this CVE to its Known Exploited Vulnerabilities (KEV) Catalog in 2023.[9]

PROOF OF CONCEPT OF A VISUAL ATTACK PLAN



Recommendation: Prioritize immediate action when dealing with critical and actively exploited vulnerabilities, which may require several steps, including:

- Identify all affected systems using comprehensive asset management and scanning
- Verify systems' vulnerability statuses against vendor advisories and deploy validated patches rapidly, using emergency change procedures when possible
- Enforce strict network containment – without delay – if a compromised IT system could provide an attack path to OT systems
- Apply firewall rules to explicitly block all unsolicited outbound traffic from impacted system to any OT system and restrict inbound network traffic to the system to only essential sources and ports
- Eliminate or secure any direct internet exposure with a VPN with MFA for necessary external access
- Monitor external threat intelligence feeds to identify relevant emerging threats and pay particular attention to campaigns affecting your industry or regional peer companies – use this intelligence to proactively deploy updated detection techniques when possible
- Maintain robust incident response readiness with documented plans designed for rapid containment of compromised systems with the intent to preventing lateral movement to OT environments and enable adequate forensic capabilities through sufficient logging and evidence collection procedures
- Enforce strong credential hygiene practices and the principle of least privilege throughout the infrastructure
- See sample rules for detection in this report.

While every organization wants to avoid security incidents, it's important to treat every security incident as an opportunity to strengthen defenses. Apply the lessons learned to review and reinforce IT and OT network segmentation policies as well as to proactively apply security hardening baselines to operating systems and applications to build resilience against future threats. See the sample rule in the gray box below for detection.

Sample rule for detecting CVE-2023-23750:

```
1  Settings > Rule Based Alerts
2  OT COMMAND RULES
3  + Add New
4
5  Rule Name: Potential CVE-2023-23750
6  Protocol: HTTP-INBOUND
7  Command Text: app?service=page/SetupCompleted
```

ACTIONS FOR YOUR TEAM

This report is intended to empower you to take necessary steps to verify your organization's security posture is properly protected. We recommend you take necessary steps to verify your organization has appropriate security controls in place.

Send this full report to your technical teams and to those accountable for cybersecurity in your organization.

Importantly, share your own information, questions and recommendations to help collectively strengthen peer cyber-physical environments. Relevant organizations include:

- Global cybersecurity community organizations such as **VirusTotal** or **Ransomwhere**
- Local government threat reporting and threat information sharing groups e.g. CERT, ENISA (see Resources on page 28)
- Honeywell Security teams
  - » If you have discovered a vulnerability that affects a product, service or solution, email us at PSIRT@honeywell.com using the following instructions:
    - Encrypt the messaging using Honeywell's public PGP key (Download PGP Key here) and include the following information:
    - Product and version
    - Description of the potential vulnerability
    - Any special configuration required to reproduce the issue
    - Step by step instructions to reproduce the issue
    - Proof of concept or exploit code, if available
    - Potential Impact
  - » For all other security issues, email us at Security@honeywell.com with the following instructions:
    - Encrypt the messaging using Honeywell's public PGP key (Download PGP Key here) and include the following information:
    - Website URL or location
    - Type of vulnerability (XSS, Injection, etc.)
    - Instructions to reproduce the vulnerability
    - Proof of concept or exploit code, including how an attacker could exploit the vulnerability

CONCLUSION AND RESOURCES

OT environment risks continue to evolve. As found in this report interval, both traditional attack vectors and variants typically found in other sectors are now impacting OT environments. As OT environments increase in sophistication and connections, it's critical to maintain cyber-physical vigilance and efficient security upkeep. The aim is to not just better manage risks, but also prevent operational disruptions. If prevention is not possible, rapid detection and response is critical.

Remember, it's not *if* your organization is attacked but *when* your organization is attacked – will you be ready? Honeywell can customize risk assessments and mitigations for your organization's OT environments.

Acknowledgements:

Special thanks to the Cybersecurity Managers from the Honeywell OT Cybersecurity Centers of Excellence in the Dubai and Singapore locations, the OT SOC analysts in the Romania location, as well as the OT Threat Intelligence team and the Honeywell Building Automation Cybersecurity Specialists in various North American locations for putting together this report. Thank you to the hundreds of OT cybersecurity specialists across Honeywell helping to protect our customers from cyber threats.

Resources:

- VirusTotal https://virustotal.com
- Mandiant Advantage Threat Intelligence https://advantage.mandiant.com
- Ransomware Live https://ransomware.live
- Ransomwhere https://ransomwhe.re
- National Vulnerability Database https://nvd.nist.gov
- Canadian Centre for Cyber Security https://www.cyber.gc.ca/en

REFERENCES

[1] Wilson Sonsini, Snapshot: The First Year of Cybersecurity Incident Filings on Form 8-K Since Adoption of New Rules, February 6, 2025

[2] ENISA, 2025 report on the state of cybersecurity in the union, December 3, 2024

[3] Office of Inspector General, EPA, Cybersecurity Concerns Related to Drinking Water Systems, November 13, 2024

[4] TechTarget, The American Water cyberattack: Explaining how it happened, October 18, 2024

[5] 90.5 WESA, Pittsburgh Regional Transit says December ransomware attack may have revealed personal data, January 7, 2025

[6] The Record, Japan Airlines Resumes operations after cyberattack delays flights, December 26, 2024

[7] Government of Canada, TA505/CL0P ransomware, July 11, 2023

[8] NIST, CVE-2023-27350 Detail, November 2023

[9] CISA, Malicious Actors Exploit CVE-2023-27350 in PaperCut MF and NG, May 11, 2023

THE FUTURE IS WHAT WE MAKE IT

Honeywell International
855 South Mint Street Charlotte,
NC 28202
www.honeywell.com

WPR-25-02-EN | 05/25

Honeywell