CTO at NCSC Summary: week ending May 19th

By Ollie Whitehouse

Published: 2025-04-12 · Archived: 2026-04-05 17:29:34 UTC

Welcome to the weekly highlights and analysis of the blueteamsec subreddit (and my wider reading). Not everything makes it in, but the best bits do.

Operationally this week nothing overly of note beyond the revelation that 400k Linux servers were compromised for financial gain!

In the high-level this week:

- CyberUK by the **UK National Cyber Security Centre** was this week in Birmingham, UK - from which there was:
    - Anne Keast-Butler keynote speech - *"Russia and Iran pose immediate threats, but China is the epoch-defining challenge."*
    - Felicity Oswald keynote speech - *"The NCSC, as the nation's technical authority on cyber security, judges that Russia, China, Iran and the DPRK continue to pose the greatest risk to the UK and our allies. "*
    - Cyber insurance industry unites to bear down on ransom payments - *"Three major UK insurance associations unite with GCHQ's National Cyber Security Centre to help reduce ransom payments made by victims of cyber crime"*
        - Guidance for organisations considering payment in ransomware incidents
    - NCSC ramps up support for those at high risk of cyber attacks ahead of election - *"NCSC service aims to help prevent political candidates and election officials from falling foul of spear-phishing, malware and other threats during major election year"*
    - National Cyber Security Centre CTO: The tech market isn't working- *"Whitehouse is expected to say that technology is changing at a rapid pace, but that regulation and legislation are not keeping pace and likely never will do. He will call for technology developers to be honest about the profound challenges they are facing in order to develop products and services that are fit for purpose and for a resilient future."*
    - Introducing the NCSC's 'Share and Defend' capability - *"'Share and Defend' is a new capability from the NCSC, designed to enable protection to the UK public and businesses from cyber attacks and cyber-enabled fraud."*
- Statement from HM Government on the adoption of UK Cyber Security Council standards - *"Support cyber security specialists at the National Cyber Security Centre (NCSC) to gain Council recognition and using the Council standards to define the skills industry will need to deliver NCSC-recognised services."*
- CHERI adoption and diffusion research - **UK Department for Science Innovation & Technology** - *"Research on the market potential for CHERI technology; a semiconductor designed to improver cyber security."*
- Learning from the mistakes of others – A retrospective review - **UK Information Commissioners Office** release - *"We have summarised several case studies from our regulatory activities to illustrate some commonly encountered*

issues and highlight where lessons might be learnt. These are not a full representation of the case and we have linked to the relevant monetary penalty notice or reprimand for further information."

- U.S. Department of the Treasury's Federal Insurance Office Launches New Partnership with the National Science Foundation on Terrorism and Catastrophic Cyber Risks - **US Department of the Treasury** announces - *"This new IUCRC will bring together the insurance sector, academic teams, the federal government, and other stakeholders to strengthen the resilience of the U.S. financial system through efforts that:*
    - *(1) help insurers to estimate risk with greater certainty, thereby improving insurance pricing, coverage, and policyholder uptake;*
    - *(2) contribute to the potential expansion of reinsurance and capital markets to help support these risks; and*
    - *(3) inform the treatment of terrorism and catastrophic cyber risks in government programs."*
- Canada joins international security partners in release of advisory, guidance on growing cyber security threat to civil society - **Canadian Centre for Cyber Security** alerts - *"In a new advisory co-authored by Canada, the United States, Estonia, Japan, Finland and the United Kingdom, cyber security agencies share new details about the ways and means foreign threat actors use for cyber attacks on civil society targets. The high-risk community of civil society organizations and individuals is defined in the report as: nonprofit, advocacy, cultural, faith-based, academic, think tanks, journalist, dissident, and diaspora organizations, communities, and individuals involved in defending human rights and advancing democracy. "*
    - Mitigating cyber threats with limited resources: Guidance for civil society - **Canadian Centre for Cyber Security** release
- Analysing the Future of Cyber Conflicts Post Russia-Ukraine War - **Predictive Defense** analyses -
- How GPS warfare is playing havoc with civilian life - **Financial Times** reports - *"Such is the fallout from a surge in the manipulation of navigation signals — modern GPS warfare — that has played havoc with civilian smartphones, planes and vessels on three continents."*
    - Related Un-jammable quantum tech takes flight to boost UK's resilience against hostile actors - UK **Department for Science Innovation & Technology** - *"A first-of-its-kind achievement as quantum navigation tech developed in the UK has been successfully tested in flight."*
- Newspaper groups warn Apple over ad-blocking plans - **Financial Times** reports - *"British newspaper groups have warned Apple that any move to impose a so-called "web eraser" tool to block advertisements would put the financial sustainability of journalism at risk."*
- Glimpse of next-generation internet - **Harvard** reports - *"The Harvard team established the practical makings of the first quantum internet by entangling two quantum memory nodes separated by optical fiber link deployed over a roughly 22-mile loop through Cambridge, Somerville, Watertown, and Boston. The two nodes were located a floor apart in Harvard's Laboratory for Integrated Science and Engineering."*
- [US] Treasury Department launches cybersecurity initiative for financial services - **ABA Banking Journal** reports- *"The Treasury Department has launched a new public-private partnership to provide what it said is a more comprehensive approach to defending the financial system from cyberattacks. The new initiative, called "Project Fortress," will involve information sharing and tools that financial institutions can use to scan for cyber vulnerabilities, according to the agency."*

- Committee on Homeland Security calls on Microsoft president testify about 'cascade of security failures, cybersecurity shortfalls' - **Committee on Homeland Security** asserts - *"However, the CSRB report revealed that Microsoft has repeatedly failed to prevent substantial cyber intrusions, causing grave implications for the security and integrity of U.S. government data, networks, and information, 6 and putting Americans—including U.S. government officials—at risk"*

- Defending Democracy

    - Justice Department vows crackdown on election-related threats - **Politico** reports - *"Top Justice Department leaders promised Monday to respond swiftly to threats against officials overseeing this year's elections and to combat the increasing use of sophisticated technology to disguise the origins of any disruptions."*

    - Hacks and propaganda: Two brothers from Moldova bring Russia's digital war to Europe - **Correctiv** investigates - *"Parallel to the war of aggression against Ukraine, Russia is stirring up sentiment in the West with fake news and cyberattacks. Two brothers from the Republic of Moldova provide the necessary technology."*

- Reporting on/from China

    - New Chinese Tianfu Cup / Pwn2Own style competition for vulnerability discovery - £2 million pound prize pool - they also have an AI competition.

    - Britain and US sound alarm over growing Chinese cyber threat - **Reuters** reports - "U.S. National Cyber Director Harry Coker told the conference that Chinese military hackers were circumventing U.S. defences in cyberspace and targeting U.S. interests at an "unprecedented scale"."

    - More subsea cables bypass China as Sino-U.S. tensions grow - **Nikkei Asia** reports - *"Once billed as a future hub for subsea networks that form vital arteries of international communication, China is expected to see only three cables laid after this year -- fewer than half the number planned for Singapore. The lack of undersea projects is also expected to weigh on the construction of data centers in the country."*

    - Tech war: US to dwarf China in advanced chip making capacity by 2032, report finds - **South China Morning Post** reports - *"The US would grow its global share of advanced chips to 28 per cent by 2032, while mainland China is expected to account for just 2 per cent"*

    - 'Superior capabilities': Chinese AI can make flooding forecast for every river on Earth - **South China Morning Post** reports - *"In the paper, the researchers wrote: "Our proposed model achieved state-of-the-art performance in cross-region streamflow forecasting tasks relative to other machine learning models and classic hydrological models."* - imagine when applied to Insurance, this is the edge.

    - China's quantum tech 'core strength' targeted by latest US trade blacklist, Chinese physicists warn - **South China Morning Post** reports - *"Updated US 'Entities List' names 22 of China's leading players in quantum research and industry among 37 of its firms and institutes targeted"*

    - Chinese scientific espionage in Germany: what next? - **Science|Business** reports - *"the Federal Public Prosecutor's Office in Germany announced the arrest of three suspected science spies who are alleged to have procured information on dual-use technologies for the Chinese secret service. They were in contact with several German universities and had signed a contract with one of them."*

- Artificial intelligence

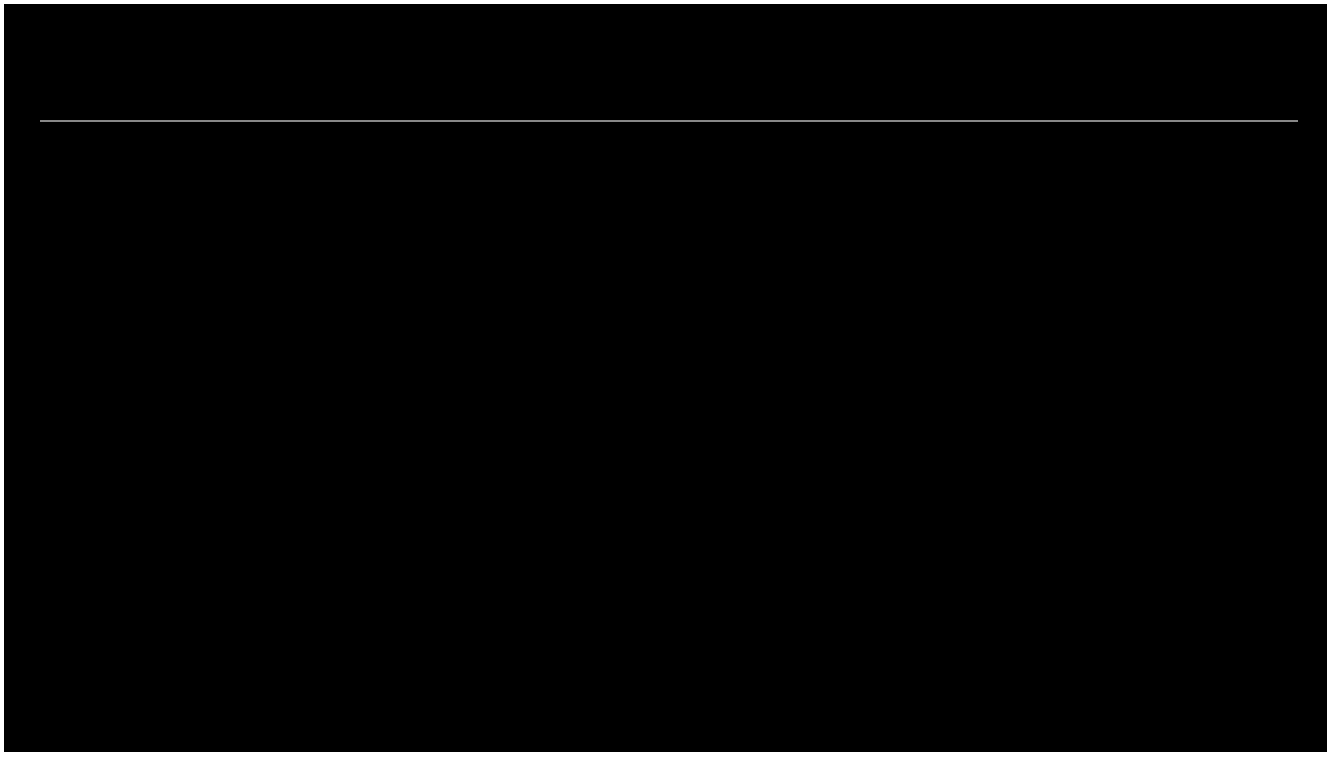
- Cyber Security of AI: call for views - UK **Department for Science Innovation & Technology** - *"The government is asking for views on a two-part intervention, including a voluntary Code of Practice on AI cyber security which will form a new global standard."*
- U.S.-China talks on AI risks set to begin in Geneva - **The Washington Post** reports - *"The talks Tuesday are aimed at preventing disastrous accidents and unintended war amid an AI arms race."*
- The Role of AI in Russia's Confrontation with the West - **CNAS** opines - *"According to public statements, the Russian government also places a significant emphasis on using AI in information and cyber operations"*
- AI systems are getting better at tricking us - **MIT Technology Review** reports - jokes about hallucinations not withstanding - *"Meta's researchers said they'd trained Cicero on a "truthful" subset of its data set to be largely honest and helpful, and that it would "never intentionally backstab" its allies in order to succeed. But the new paper's authors claim the opposite was true: Cicero broke its deals, told outright falsehoods, and engaged in premeditated deception. Although the company did try to train Cicero to behave honestly, its failure to achieve that shows how AI systems can still unexpectedly learn to deceive, the authors say. "*
- Japan to launch U.S.-inspired defense R&D center with eye on AI - **Nikkei Asia** reports - *"The center will also research new, more sensitive methods to detect submarines from a distance using subatomic particles and electromagnetic waves. Conventional sonar has become less effective following technological improvements that have made subs quieter."*
- Adversary use of Artifical Intelligence and LLMs and Classification of TTPs - *"an attempt to organize known use of artificial intelligence by cyber threat actors and to map and track those techniques."*

- Cyber proliferation
  - Ex-Variston zero-day experts regroup at Paradigm Shift - **Intelligence Online** reports - *"The fallout of Google's accusations has left the Spanish cyber intelligence firm floundering and its zero-day vulnerability hunters leaving to new ventures."*
- Bounty Hunting
  - Rewards for Justice – Reward Offer for Information on North Korean IT Workers - **US Department of State**
  - Security expert detained in court for 'hacking 400,000 households' wall pads and distributing video' - **Donga** reports - *"Court sentenced to 4 years in prison*
    for attempting to sell private videos hacked into 638 apartment complexes across the country"
  - Developer of Tornado Cash goes to jail for laundering billions of dollars in cryptocurrency - **de Rechtspraak** reports - *"The East Brabant court has sentenced a 31-year-old Russian, living in Amstelveen, to a prison term of 5 years and 4 months. He developed and maintained the software tool Tornado Cash, which laundered a total of more than two billion US dollars. "*
  - Two Brothers Arrested for Attacking Ethereum Blockchain and Stealing $25M in Cryptocurrency - **US Department of Justice**
  - Democratic People's Republic of Korea Leverages U.S.-Based Individuals to Defraud U.S. Businesses and Generate Revenue - **FBI**

Reflections this week are around kind people. I had a number of you come up to me at CyberUK and thank me for producing this each week. Nearly all of you wondered where I got the time, did I sleep etc. I think I retorted to most of you I

am sufficiently neurodiverse coupled with it being a labour of love. Anyway, very kind of all of you who did speak to me.

My keynote on market failures and incentives is also something I have trailed here in various guises. The video can be seen here:



Think someone else would benefit? Share:

Share

All attribution is by others and not the UK Government unless specifically stated as such, please see the legal text at the end.

Have a lovely Friday..

Ollie

Who is doing what to whom and how allegedly.

Ukrainian Government alleges a concerted campaign which is noteworthy due to the leveraging of diversified communications channels for initial access as much as anything.

> - use of legitimate software for deception: hackers tried to disguise spyware as legitimate apps, such as the situational awareness system “Kropyva”;
> - spreading malware through popular messengers: hackers used popular messengers like Signal and Telegram, imitating cybersecurity guidelines issued by CERT-UA;
> - quick reaction and adaptation: hackers quickly reacted to new defense measures and developed new attack vectors to bypass them;
> - targeted Windows software: most messenger-based attacks targeted Windows software, as many Ukrainian servicemen use PC versions of the messengers;

> - decoy files: hackers attempted to spread malware disguised as certificate updates to the “DELTA” situational awareness complex, using Zip or Rar archives.

https://cip.gov.ua/en/news/rosiiski-khakeri-aktivizuvali-ataki-na-mobilni-pristroyi-ukrayinskikh-viiskovikh-doslidzhennya-derzhspeczv-yazku

Filip Jurčacko alleges that a Russian state based actor has evolved their implants. Noteworthy due to the use of steganography.

> - [We] discovered two previously unknown backdoors – LunarWeb and LunarMail – used in the compromise of a European MFA and its diplomatic missions.
> - LunarWeb, deployed on servers, uses HTTP(S) for its C&C communications and mimics legitimate requests, while LunarMail, deployed on workstations, is persisted as an Outlook add-in and uses email messages for its C&C communications.
> - Both backdoors employ the technique of steganography, hiding commands in images to avoid detection.
> - Both backdoors utilize a loader that uses the DNS domain name for decryption of the payload, share portions of their codebases, and have the unusual capability of being able to execute Lua scripts.
> - The loader can have various forms, including trojanized open-source software, demonstrating the advanced techniques used by the attackers.

https://www.welivesecurity.com/en/eset-research/moon-backdoors-lunar-landing-diplomatic-missions/

Volexity alleges that a China-based threat actor was behind (some) the Palo Alto attacks..

> - Shortly after the advisory for CVE-2024-3400 was released, scanning and exploitation of the vulnerability immediately increased. The uptick in exploitation appears to have been associated with UTA0218 or another threat actor that had early access to the exploit prior to proof-of-concept code being made public.
> - Multiple organizations were exploited in late March 2024 with simple commands designed to place zero-byte files on the systems in what appears to be an effort to validate vulnerable devices. Volexity did not observe follow-on activity from threat actors in most of these cases.
> - Exfiltration of the firewall’s running configuration was the most commonly observed post-exploitation activity across devices spanning numerous verticals and geographic regions. This was observed in the earliest exploitation by UTA0218, and by future unrelated threat actors after public proof-of-concept code was made available.
>
> …
>
> Volexity assesses with moderate confidence that UTA0218 is a China-based threat actor based on the targeting and infrastructure used for this campaign.

https://www.volexity.com/blog/2024/05/15/detecting-compromise-of-cve-2024-3400-on-palo-alto-networks-globalprotect-devices/

Pierre Lee and **Cyris Tseng** provide an update on this alleged Chinese campaign and how it continues to evolve. It highlights that threat actors are increasingly evolving tradecraft to evade detections. Note the anti-memory scanning techniques!

> - Earth Hundun is known for targeting the Asia-Pacific and now employs updated tactics for infection spread and communication.
> - This report details how Waterbear and Deuterbear operate, including the stages of infection, command and control (C&C) interaction, and malware component behavior.
> - Deuterbear, while similar to Waterbear in many ways, shows advancements in capabilities such as including support for shellcode plugins, avoiding handshakes for RAT operation, and using HTTPS for C&C communication.
> - Comparing the two malware variants, Deuterbear uses a shellcode format, possesses anti-memory scanning, and shares a traffic key with its downloader unlike Waterbear.
> - The evolution of Waterbear into Deuterbear indicates the development of tools for anti-analysis and detection evasion in Earth Hundun's toolbox.

https://www.trendmicro.com/en_us/research/24/e/earth-hundun-2.html

Genians details an alleged North Korean campaign. The novelty here is the file format used to achieve code execution which may be a blind spot for some.

> - Disguised as a public official in the North Korean human rights field and searched for attack targets through Facebook
> - After a personal approach through Facebook Messenger, a brief greeting and conversation begin.
> - Share malicious URL link address by pretending to be a specific document file
> - Observe MSC-based threats through OneDrive cloud service
> - Identification of ReconShark-like malware from Kimsuky group

https://www-genians-co-kr.translate.goog/blog/threat_intelligence/facebook?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en-US&_x_tr_pto=wapp

Symantec alleges North Korea has expanded to include Linux as a target operating system of this campaign.

> [We] uncovered a new Linux backdoor developed by the North Korean Springtail espionage group (aka Kimsuky) that is linked to malware used in a recent campaign against organizations in South Korea.
>
> The backdoor (Linux.Gomir) appears to be a Linux version of the GoBear backdoor, which was used in a recent Springtail campaign that saw the attackers deliver malware via Trojanized software installation packages. Gomir is structurally almost identical to GoBear, with extensive sharing of code between malware variants.

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/springtail-kimsuky-backdoor-espionage

QiAnXin Threat Intelligence Center reports on an alleged North Korean supply chain to get crypto assets. Note this appears to a continuation of a DreamJob-esq campaign.

> [We] found that the attackers continued to carry out frequent attacks after being disclosed at the end of last year, and the victims were mainly developers in the blockchain industry. Attackers create false identities on work platforms (such as LinkedIn, Upwork, Braintrust, etc.), pretend to be employers, independent developers, or startup founders, and post job information with generous rewards or urgent tasks. The job content is usually

> software development. Or problem fixed. This job information will attract developers who actively search for it, or it will be presented to the target group through the push mechanism of the platform. While discussing the job description, the attackers tried to convince the candidates to run the code they provided on their devices. Once the applicant runs the program without suspicion, the malicious JS code inserted will steal sensitive information related to virtual currency on the infected device and implant other malware.

https://mp-weixin-qq-com.translate.goog/s/84lUaNSGo4lhQlpnCVUHfQ?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en-US&_x_tr_pto=wapp

Obsidian observe some strong TTPs in this alleged Iranian aligned operation. These should provide some real detection opportunities.

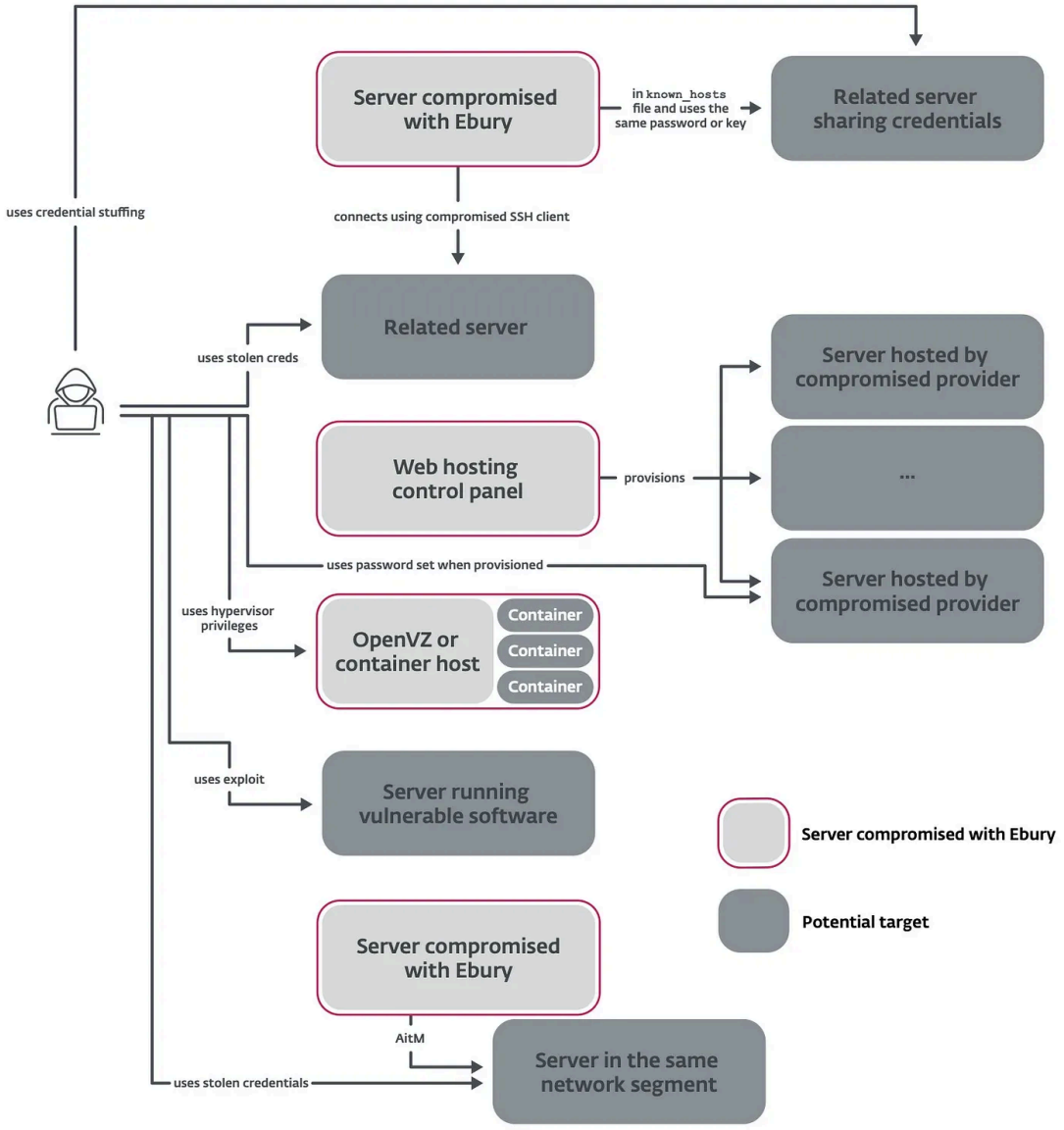
> [We] observed a set of unique characteristics across several targeted attacks, distinguishing them from others of a similar kind.
>
> - **Residential Proxy Usage:** Phishing kits and services are taking advantage of proxy networks that utilize a variety of residential IPs. To evade detection and get past conditional access policies, attackers can appear in the same city as a victim while also coming from a residential ISP such as Comcast, Cox, T-Mobile, Verizon, etc. This gives attackers an advantage as opposed to coming from IP space associated with private VPNs or hosting infrastructure which is easier for defenders to identify. As you can imagine, this muddies the waters when performing detection engineering, security operations, and incident response.
>
> - **"Zscaler Inc." ISP Minted a Malicious Session.** Residential proxy networks consist of willing and unwilling parties leasing their bandwidth and IP to other users. There are a variety of ways in which these networks are built, deployed, and used which was covered extensively in a **blog post** by Sekoia. The victim organization was not a paying customer of Zscaler but we see this ISP appear in one of the compromised login sequences that matched those of other true positives that all went through residential proxy IPs. To the best of our knowledge, Zscaler can be set up in a VPN mode via Zscaler Client Connector. This can technically route all traffic on a machine through Zscaler infrastructure, potentially including traffic from a residential proxy agent or traffic via a compromised host. The residential proxy agents we tested were able to distinguish residential IPs from infrastructure IPs and only route traffic via the IPs they classified as residential. However, this was not an exhaustive test so we can not completely rule out the possibility that the Zscaler IP came from a voluntary proxy agent. Regardless of it being a residential proxy agent or a compromised host, residential IPs mixed with security gateway IPs, for obvious reasons, can complicate matters further…
>
> - **Outdated User Agent.** In addition to the use of residential proxies, the attackers used an outdated Chrome user agent released in 2019. While detecting phishing through residential proxies poses a challenge, this simple IOC has a very high success rate in identifying these attacks.
>
> .

https://www.obsidiansecurity.com/blog/emerging-identity-threats-the-muddy-waters-of-residential-proxies/

Marc-Etienne M.Léveillé details a decade old criminal campaign which continues to thrive I think it is fair to say. The alleged compromise of kernel.org for three years will be of concern.

> - Ebury actors have been pursuing monetization activities subsequent to our 2014 publication on Operation Windigo, including the spread of spam, web traffic redirections, and credential stealing.

- Additionally, we have confirmed that operators are also involved in cryptocurrency heists by using AitM and credit card stealing via network traffic eavesdropping, commonly known as server-side web skimming.
- Over the years, Ebury has been deployed to backdoor almost 400,000 Linux, FreeBSD, and OpenBSD servers, and more than 100,000 were still compromised as of late 2023.
- We uncovered new malware families authored and deployed by the gang for financial gain, including Apache modules and a kernel module to perform web traffic redirection.
- In many cases, Ebury operators were able to gain full access to large ISPs and well-known hosting providers. They used that access to deploy Ebury on the partial or complete server infrastructure hosted by that provider.
- Ebury also compromised the infrastructure of other threat actors, including Vidar Stealer and many others, to steal data stolen by those other groups and copycat competing operations to blur attribution attempts.
- Ebury operators also used zero-day vulnerabilities in administrator software to compromise servers in bulk.
- The data we obtained confirmed a number of suspected victims, including the compromise of kernel.org from 2009 to 2011.
- We provide a set of tools and indicators to help system administrators determine whether their systems are compromised by Ebury.



https://www.welivesecurity.com/en/eset-research/ebury-alive-unseen-400k-linux-servers-compromised-cryptotheft-financial-gain/

Insikt Group have discovered what we shall call a scaled campaign.

> Insikt Group discovered an extensive and multi-faceted campaign, attributed to Russian-speaking threat actors likely located in the Commonwealth of Independent States (CIS), abusing a legitimate GitHub profile to impersonate legitimate software, such as 1Password, Bartender 5, and Pixelmator Pro, among others, and distribute various malware families focused on stealing personal information from unsuspecting victims. Some malware families observed in this campaign, like Atomic macOS Stealer (AMOS), Vidar, Lumma, and Octo, use shared command-and-control (C2) systems, showing a complex, coordinated cyberattack strategy. The presence of multiple malware variants suggests a broad cross-platform targeting strategy, while the overlapping C2 infrastructure points to a centralized command setup — possibly increasing the efficiency of the attacks. This demonstrates a technique where attackers employ multiple variants in cross-platform attacks to boost their campaigns' success rates.

> - The campaigns observed in this investigation demonstrate a strategic targeting approach across a spectrum of operating systems and computer architectures, reflecting the threat actors' broad goals and their adaptability to evolving technological landscapes.
> - GitHub, a widely utilized platform for collaborative software development, has been utilized as a vector for the propagation of the infostealer AMOS, among other infostealers, masquerading as legitimate applications. This campaign highlights the abuse of legitimate internet services (LIS), underscoring an intention to undermine organizations' trust in such services.
> - Despite having access to a wide range of premium cybercriminal tools and techniques, the threat actors identified in this campaign use free and web-based infrastructure, like FileZilla servers, as a mechanism for malware delivery, abusing these legitimate channels to disseminate various malicious payloads to victims' devices. This tactic showcases a deliberate effort to obfuscate malicious activity within seemingly benign infrastructure.
> - The presence of Russian-language artifacts within the analyzed HTML code suggests potential linguistic and geographical affiliations of threat actors associated with the development or deployment of the observed malware

https://go.recordedfuture.com/hubfs/reports/cta-2024-0514.pdf

Who had OCR in implants on their bingo card? **Sanseo** details an example where it is the case. So photos of you passwords is not a mitigation of exfiltration.

> The malware newly discovered this time utilizes the open-source OCR engine Tesseract. Tesseract extracts texts from images using deep learning techniques. The malware used in the attack reads images stored on the infected systems and extracts strings using the Tesseract tool. If the extracted strings contain any phrases related to passwords or cryptocurrency wallet addresses, the malware exfiltrates those images.

https://asec.ahnlab.com/en/65426/

Phil Stokes released this earlier this month but I missed it. It is worth covering because of the pace of pivot by the threat actor. Where there is an incentive threat actors will adapt - the 🐱 and 🐭 games begin!

> It's been little more than a week since Apple rolled out an unprecedented 74 new rules to its XProtect malware signature list in version 2192. A further 10 rules were appended in version 2193 on April 30th. Cupertino's security team were clearly hoping that a concerted effort would serve to disrupt prolific adware distributor Adload's assault on macOS devices. Those behind the adware, however, appear to have pivoted quickly as dozens of new Adload samples are already appearing that evade Apple's new signatures.

https://www.sentinelone.com/blog/macos-adload-prolific-adware-pivots-just-days-after-apples-xprotect-clampdown/

How we find and understand the latent compromises within our environments.

Adan provides an open source project which will provide value to those living in the AWS eco-system by reducing some of the overhead.

> I've developed another project, HoneyTrail, to support the deployment of deception solutions. Designed specifically for AWS users, HoneyTrail adds a layer of deception without a complicated setup process. It's a straightforward Terraform that integrates honeypots directly within AWS, eliminating the need for additional

> setups or dependencies. It offers functionality similar to what AWS presented here, but it utilizes Terraform and does not need Security Hub, which is an extra cost.

https://medium.com/@adan.alvarez/deterring-attackers-with-honeytrail-deploying-deception-in-aws-6b5977afa784

https://github.com/adanalvarez/HoneyTrail

Rad provides this which when combined with the right action will provide a canary that will fire.

gist.github.com/radk2/45e729f5859d76197d8f7e6b53dd6d71

Stephan Berger shows that anti-forensics is really a thing for some threat actors.

> stumbled upon a ‘cleaner’ script, which we will examine in this short blog post.
>
> ..
>
> Last, the script changes the name of the Splashtop firewall rule with the command Set-NetFirewallRule. The comment inside the code reads, translated from Russian to English: *Change the name and description of the rule to “Cast to Device streaming server (HTTP-Streaming-In)*:

https://dfir.ch/posts/cleanup_script_rmm/

Interesting forensics source for Windows environment which I suspect a lot don’t know about.

> - Used by Windows servers to aggregate client usage data by role and products on a server.
> - Used to assist Administrators quantify requests from client computers for roles and services, as described by Microsoft
> - Installed by default on
>   - Windows Server 2012, 2012 R2, 2016, 2019, 2022
> - Collects data going back 3 years

https://www.thedfirspot.com/post/sum-ual-investigating-server-access-with-user-access-logging

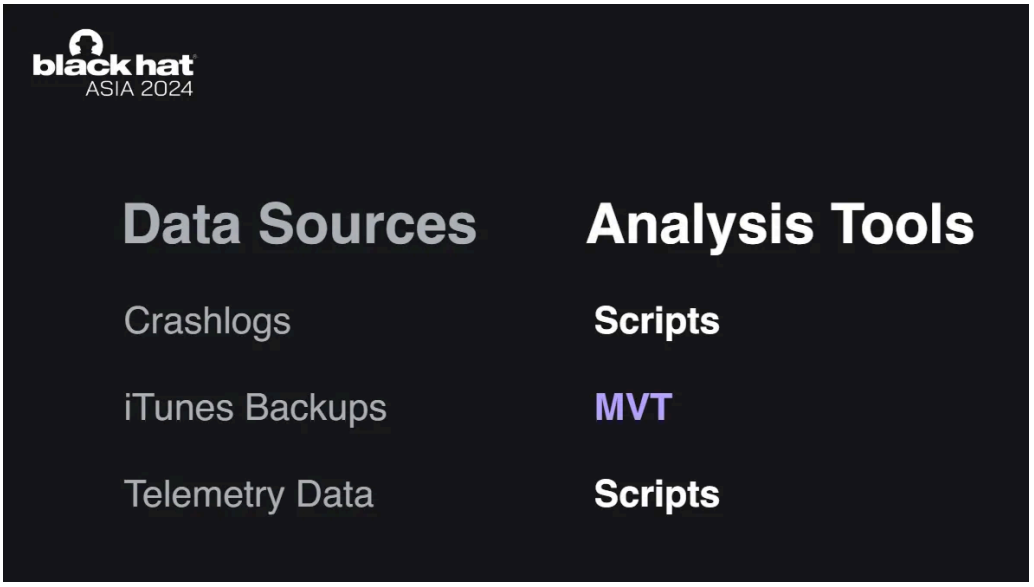
Squiblydoo shows the scale of illicit certificate use by this threat actor. Hints we might need to improve the process.

> Since 2023, I have documented *another* 50 certificates leveraged by SolarMarker: bringing us to 100 certificates known to be abused by the actor. The purpose of this blog-post is to continue to expand awareness of impostor certs by reviewing the impostor certs used by SolarMarker as a case study.

https://squiblydoo.blog/2024/05/13/impostor-certs/

How we proactively defend our environments.

Matthias Frielingsdorf walks through end to end analysis NSO iOS samples.



https://i.blackhat.com/Asia-24/Asia-24-Frielingsdorf-YouShallNotPassAnalysing.pdf

Yakir Kadkoda and **Assaf Morag** show that if you are an APT and you look for it you might find a way in sitting on the Internet for an initial foothold. Highlights the importance of tokens as a means for an authentication.

> During our research, we found credentials within a git commit by a Microsoft employee, which granted us access to an internal Azure Container Registry used by Azure. This registry contains images critical to various Azure projects, such as Azure IoT Edge, Akri, and Apollo. The exposed token provided privileged access, allowing us to download private images and upload/overwrite images.
>
> ..
>
> During our investigation, we discovered several instances where Red Hat employees unintentionally exposed tokens for internal Red Hat container registries containing highly sensitive data linked to vital corporate functions. These tokens grant both pull and push privileges, posing substantial risks to the company.
>
> ..
>
> During our research, we discovered credentials for the internal container registry (quay.io/tigera) exposed in a Git commit of other company. This registry contains images from various Tigera projects, such as Calico, and more.

https://www.aquasec.com/blog/github-repos-expose-azure-and-red-hat-secrets/

How they got in and what they did.

Key Tronic Corporation is a technology company who's core products initially included keyboards, mice and other input devices. Sounds like ransomware, but given the types of devices just imagine if it had been supply chain!

> On May 6, 2024, Key Tronic Corporation (the "Company") detected unauthorized third party access to portions of its information technology ("IT") systems. Upon detection of this outside threat, the Company activated its cyber incident procedure to investigate, contain, and remediate the incident, including beginning an investigation with external cybersecurity experts and notifying law enforcement.

https://www.board-cybersecurity.com/incidents/tracker/20240509-key-tronic-corp-cybersecurity-incident/

Our attack surface.

Bit of an ‘if’, but widely used..

> If pdf.js is used to load a malicious PDF, and PDF.js is configured with `isEvalSupported` set to `true` (which is the default value), unrestricted attacker-controlled JavaScript will be executed in the context of the hosting domain.

https://github.com/advisories/GHSA-wgrm-67xf-hhpq

Attack capability, techniques and trade-craft.

Interesting write up on the various technical implementation details

> - Technique one: The IFUNC feature of GLIBC
> - Technique two: Concealing characters using Radix Tree
> - Technique three: Obtaining all dependency information
> - Technique Four: Hooking Functions from Other Dependency Libraries

https://medium.com/@knownsec404team/techniques-learned-from-the-xz-backdoor-74b0a8d45c30

Expect malicious use in 3..2..

> Reverst is a (load-balanced) reverse-tunnel server and Go server-client library built on QUIC and HTTP/3.
>
> - Go Powered: Written in Go using quic-go
> - Compatible: The Go `client` package is built on `net/http` standard-library abstractions
> - Load-balanced: Run multiple instances of your services behind the same tunnel
> - Performant: Built on top of QUIC and HTTP/3

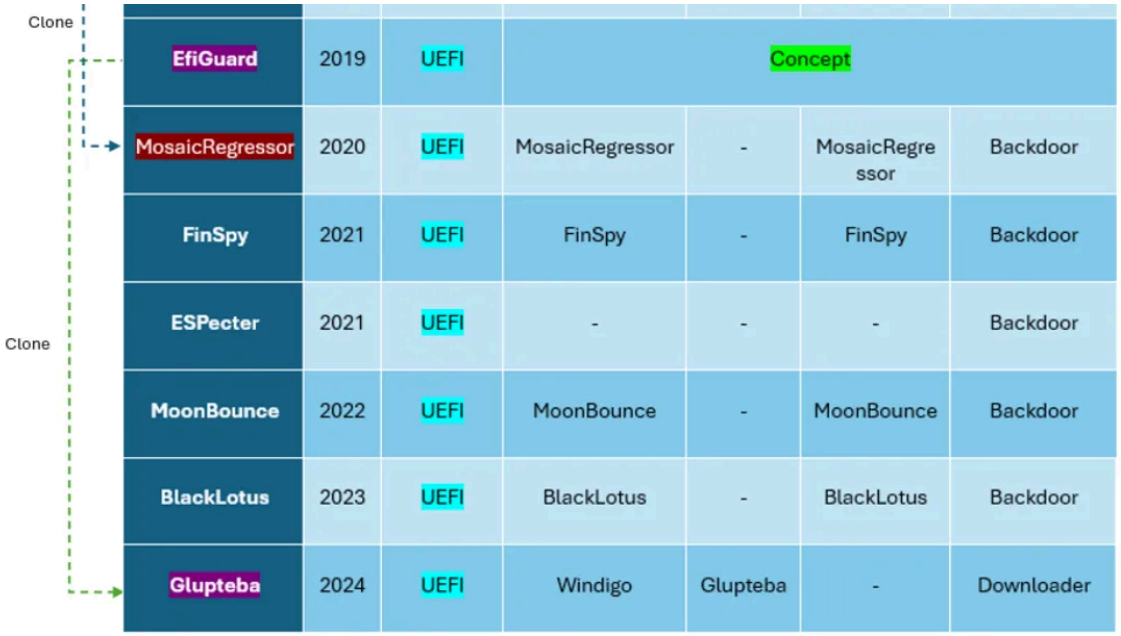
https://github.com/flipt-io/reverst/

From a Chinese researcher.

> darkPulse is a shellcode Packer written in Go. It is used to generate various shellcode loaders. Currently, it is free of tinder, 360, and 360 core crystal.

https://github.com/fdx-xdf/darkPulse

Lovely summary here.



https://artemonsecurity.blogspot.com/

What is being exploited.

Boris Larin and **Mert Degirmenci** show that zero days sometimes float around in semi open source and that criminals do have some sort of supply mechanism.

> In early April 2024, we decided to take a closer look at the Windows DWM Core Library Elevation of Privilege Vulnerability CVE-2023-36033, which was previously discovered as a zero-day exploited in the wild. While searching for samples related to this exploit and attacks that used it, we found a curious document uploaded to VirusTotal on April 1, 2024.
>
> After sending our findings to Microsoft, we began to closely monitor our statistics in search of exploits and attacks that exploit this zero-day vulnerability, and in mid-April we discovered an exploit for this zero-day vulnerability. We have seen it used together with QakBot and other malware, and believe that multiple threat actors have access to it.

https://securelist.com/cve-2024-30051/112618/

Antonis Terefos gives a good example of poor socio-technical design and the security implications of it. Also of note is the wide use of this technique..

> Check Point Research discovered that samples from EXPMON produced unusual behavior when executed with Foxit Reader compared to Adobe Reader. The exploitation of victims occurs through a flawed design in Foxit Reader, which shows as a default option the “OK,” which could lead the majority of the targets to ignore those messages and execute the malicious code. The malicious command is executed once the victim “Agrees” to the default options twice.
>
> Once clicking “OK“, the target comes across a second pop-up. If there were any chance the targeted user would read the first message, the second would be “Agreed” without reading. This is the case that the Threat Actors are taking advantage of this flawed logic and common human behavior, which provides as the default choice the most “harmful” one.

> [We] collected a plethora of malicious PDF files, taking advantage of the specific exploit targeting Foxit Reader users. Despite the majority of sandboxes and VirusTotal failing to trigger the exploit, given Adobe's prevalence as the primary PDF Reader, numerous files from previous campaigns remained unretrieved.

https://research.checkpoint.com/2024/foxit-pdf-flawed-design-exploitation/

Low level tooling and techniques for attack and defence researchers…

Air provides useful work aid for those who haven't moved to Ghidra.

> **SourceSync** is both a set of plugins for synchronisation between debugger and decompiler and a library for generating pdb from decompiler data. In the case of plugins, it establishes a connection between the debugger (Windbg, client) and the decompiler (Ida Pro, server) to dynamically generate pdb for functions in the current thread call stack that belong to the decompiled module.

https://github.com/Air14/SourceSync

Some other small (and not so small) bits and bobs which might be of interest.

- Aggregate reporting
    - ESET APT Activity Report Q4 2023–Q1 2024
    - The 471 Cyber Threat Report 2024
- ODNI Releases Intelligence Community Policy Framework for Commercially Available Information
- Moving beyond linearity in academic-policymaking impact claims of futures and foresight
- Covert Connections: The LinkedIn Recruitment Ruse Targeting Defense Insiders
- Artificial intelligence
    - A framework for large language model evaluations created by the UK AI Safety Institute.
    - Oracle community knowledge base based on LLM
    - SoK: Where to Fuzz? Assessing Target Selection Methods in Directed Fuzzing - *"Our analysis provides new insights for target selection in practice: First, we find that simple software metrics significantly outperform other methods, including common heuristics used in directed fuzzing, such as recently modified code or locations with sanitizer instrumentation. Next to this, we identify language models as a promising choice for target selection"*
    - Does Fine-Tuning LLMs on New Knowledge Encourage Hallucinations?
- Books
    - *Nothing this week*
- Events
    - *Nothing this week*

Unless stated otherwise, linked or referenced content does not necessarily represent the views of the NCSC and reference to third parties or content on their websites should not be taken as endorsement of any kind by the NCSC. The NCSC has no

control over the content of third party websites and consequently accepts no responsibility for your use of them.

This newsletter is subject to the NCSC website terms and conditions which can be found at https://www.ncsc.gov.uk/section/about-this-website/terms-and-conditions and you can find out more about how will treat your personal information in our privacy notice at [https://www.ncsc.gov.uk/section/about-this-website/privacy-statement.](https://www.ncsc.gov.uk/section/about-this-website/privacy-statement)
