CTO at NCSC Summary: week ending October 29th

By Ollie Whitehouse

Published: 2025-04-12 · Archived: 2026-04-02 12:01:57 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.

Firstly, welcome to the new home but same format for those that have followed here from the old Substack. As I've moved roles we had to move due to me working for the UK Government. A quick thank you to the NCSC's communications, legal and policy teams who made all the magic happen very quickly. Be sure to check out the bottom of the legal language.

Operationally this week you will see two things have been driving the agenda - the Okta breach (see reporting below) and the at scale router compromises. Clean up around the latter continues…

In the high-level this week:

- The (US) National Cyber Incident Response Plan (NCIRP) - *CISA is leading an effort to update the National Cyber Incident Response Plan (NCIRP) by the end of 2024, as directed in the 2023 National Cybersecurity Strategy*
- CYBERCOM executes internal coordinated defensive cyber activity - *Focusing distinctly on DoD networks and systems, CYBERCOM globally deployed defensive cyber professionals to search for, identify, mitigate, and publicly share known malware and associated variations targeting DoD-network infrastructure. INCCA provides defensive cyber teams with an opportunity to improve processes, readiness, and coordination with our broader unified action partners.*
- European Council sets out vision for protecting fundamental rights in the digital world - *The text reaffirms that fundamental rights apply equally online and offline and that everyone should have the opportunity and support to acquire basic digital skills in order to be able to comprehend and exercise their rights.*

  Justice Department Announces Court-Authorized Action to Disrupt Illicit Revenue Generation Efforts of Democratic People's Republic of Korea Information Technology Workers - North Koreans getting remote jobs in US firms

  - related North Korean programmers used a hosted laptop to freelance online, says FBI
- Measures taken following the unprecedented cyber-attack on the ICC - *As part of broader assessment into potential actions by threat actors, the Court has also identified that disinformation campaigns targeting the ICC and its officials may be anticipated to be launched in an effort to tarnish the ICC image a*nd delegitimize its activities.

  - Additionally we had France condemns the cyber attack against the International Criminal Court - *It also strongly condemns the criminal proceedings initiated in Russia against the Court's staff – the President, First Vice-President, Prosecutor, judges preparing cases for trial who are involved in the situation in Ukraine, and a trial judge.*
- Protecting Civilians Against Digital Threats During Armed Conflict: Recommendations to states, belligerents, tech companies, and humanitarian organizations - *The Board's final report presents 4 guiding principles and a set of 25*

concrete recommendations addressed to belligerents, states, tech companies, and humanitarian organizations to prevent or mitigate digital threats to civilian populations.

- The Economics of Ransomware Attacks on Integrated Supply Chain Networks - *we show that by targeting one firm in the network the criminals can potentially hold multiple firms to ransom* - something to consider from this.
- Summary of the threat targeting local (French) authorities - *From January 2022 to June 2023, ANSSI handled 187 incidents in this area. If the profit objective is, by far, the primary motivation of attackers who target local authorities, the latter can however be the subject of attacks for the purposes of destabilization, or even compromise linked to state espionage operations .*
- China
    - This is the state of generative AI in China - *Domestically, Chinese companies are facing a particularly complex regulatory landscape, characterized by rapidly evolving rules and standards for the development and deployment of generative AI products. China's internet regulators are well ahead of their counterparts in the U.S. in pursuing "vertical" regulatory approaches to AI in general and generative AI in particular, issuing interim regulations on generative AI in July.*
    - Full text of Xi Jinping's keynote speech at 3rd Belt and Road Forum for Int'l Cooperation - *Fifth, advancing scientific and technological innovation. China will continue to implement the Belt and Road Science, Technology and Innovation Cooperation Action Plan, hold the first Belt and Road Conference on Science and Technology Exchange, increase the number of joint laboratories built with other parties to 100 in the next five years, and support young scientists from other countries to work on short-term programs in China. At this Forum, China will put forward the Global Initiative for Artificial Intelligence (AI) Governance.*
    - How Do The Chinese Ciphers Compare with NIST Standards? - slow is the answer but that could be due to lack of hardware acceleration.
    - China crackdown on cyber scams in Southeast Asia nets thousands but leaves networks intact - *Regional and Chinese authorities have netted thousands of people in a crackdown, but experts say they are failing to root out the local elites and criminal networks that are bound to keep running the schemes.*
- Artificial intelligence
    - Frontier AI: capabilities and risks – discussion paper - published by the UK including the Annex B: Safety and Security Risks of Generative Artificial Intelligence to 2025
    - UK's DSIT opens AI Fairness Innovation Challenge - *The Department for Science, Innovation, and Technology (DSIT) has launched a competition offering £400,000 for investment in projects to tackle bias and discrimination in AI.*
    - Decomposing Language Models Into Understandable Components - *using a large language model to generate short descriptions of the small model's features, which we score based on another model's ability to predict a feature's activations based on that description*
    - Microsoft announces A$5 billion investment in computing capacity and capability to help Australia seize the AI era - *In addition, Microsoft will collaborate with the Australian Signals Directorate (ASD) on an initiative called the Microsoft-Australian Signals Directorate Cyber Shield (MACS), aimed at improving protection from cyber threats for Australian residents, businesses and government entities.*

    - European Data Protection Supervisor Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legislative developments - *the EDPS reiterates that AI systems already in use at the date of applicability of the AI Act, including AI systems which are components of EU large-scale IT systems, should not be exempted from the scope of the AI Act. Instead, they should comply with the AI Act requirements from its date of applicability.*

- Cyber proliferation

    - Intellexa: Irish-linked spyware used in 'brazen attacks' - *The Irish government is set to investigate a digital surveillance alliance that has been accused of letting its smartphone spyware "run wild across the world", BBC News NI understands.*

    - Israeli Cyber Arms and Intelligence Firms Like NSO Aiding Israeli Efforts - *From facial recognition to open source intelligence and offensive cyber, firms such as NSO, Rayzone and others like AnyVision helped map and track hostages, casualties*

Reflections this week are how liberating it is to move to an organisation (the NCSC) who work on true national strategic intent. I knew I would find it fulfilling but some of the opportunities (and challenges) which I have had exposure to in the first week along with the clear sense of mission make it truly motivating..

On the interesting job/role front (thanks to those sending me these):

- Operational and Cyber Resilience Manager at the Financial Conduct Authority in the UK
- Principal Cyber Advisor to the Secretary of the Navy in the USA

Enjoying this? Don’t get via e-mail? Subscribe:

Think someone else would benefit? Share:

Share

Attribution is by others.

Have a lovely Thursday

Ollie

Who is doing what to whom and how.

Some data as to the scale of this challenge..

> To date in 2023, more than 100 companies across 18 industries had access to their IT infrastructure, cloud environments, networks, or applications sold on Russian hacking forums.

https://flare.io/learn/resources/blog/threat-spotlight-initial-access-brokers-on-russian-hacking-forums/

Insider threat personified by this reporting from our friends in Ukraine.

> the group includes traitor officers of the former Security Service of Ukraine Dept. in the Autonomous Republic of Crimea, who started ministering to Russian federal security back in 2014.

https://cip.gov.ua/en/news/rosiiske-ugrupuvannya-gamaredon-suttyevo-zbilshilo-kilkist-kiberoperacii-prote-voni-ne-taki-uspishni-yak-ranishe

Matthieu Faou gives us reporting that shows this threat actor has continued the trend of exploiting web vulnerabilities in email servers via email.

> Exploitation of the XSS vulnerability, assigned CVE-2023-5631, can be done remotely by sending a specially crafted email message.
>
> We believe with low confidence that Winter Vivern is linked to MoustachedBouncer, a sophisticated Belarus-aligned group that we first published about in August, 2023.

https://www.welivesecurity.com/en/eset-research/winter-vivern-exploits-zero-day-vulnerability-roundcube-webmail-servers/

Bit of a pulse check on activity from the Hermit Kingdom..

> The Kimsuky group's activities in August 2023 showed a notable surge in the BabyShark type, while the activities of other types were relatively low.

https://asec.ahnlab.com/en/57938/

Canadian government reporting on Chinese activity in country.

> Global Affairs Canada's (GAC) Rapid Response Mechanism (RRM) Canada has detected a 'Spamouflage' campaign connected to the People's Republic of China. Beginning in early August 2023 and accelerating in scale over the September long-weekend, a bot network left thousands of comments in English and French on the Facebook and X/Twitter accounts of Canadian Members of Parliaments (MPs).

https://www.canada.ca/en/global-affairs/news/2023/10/rapid-response-mechanism-canada-detects-spamouflage-campaign-targeting-members-of-parliament.html

https://www.aspistrategist.org.au/ccp-using-information-operations-to-harass-canadian-politicians/

I mistakenly missed this reporting off last week on Iranian activity against regional governments.

> The Iranian Crambus espionage group (aka OilRig, APT34) staged an eight-month-long intrusion against a government in the Middle East between February and September 2023. During the compromise, the attackers stole files and passwords and, in one case, installed a PowerShell backdoor (dubbed PowerExchange) that was used to monitor incoming mails sent from an Exchange Server in order to execute commands sent by the attackers in the form of emails, and surreptitiously forwarded results to the attackers. Malicious activity occurred on at least 12 computers and there is evidence that the attackers deployed backdoors and keyloggers on dozens more.
>
> In addition to deploying malware, the attackers made frequent use of the publicly available network administration tool Plink to configure port-forwarding rules on compromised machines, enabling remote access via the Remote Desktop Protocol (RDP). There is also evidence the attackers modified Windows firewall rules in order to enable remote access.

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/crambus-middle-east-government

PwC report suggests that someone is doing data collection.

> - Between 2022 and 2023, the threat actor has conducted strategic web compromises to embed JavaScript which fingerprints website visitors and captures victim user location, device information, and time of visits. Targeting of these attacks have focused primarily on the maritime, shipping and logistics sectors, with some victims being served follow-on malware which we have named IMAPLoader.

> - IMAPLoader is a .NET malware that has the ability to fingerprint victim systems using native Windows utilities and acts as a downloader for further payloads. It uses email as a C2 channel and is able to execute payloads extracted from email attachments and is executed via new service deployments.
> - We have previously observed Yellow Liderc developing .NET malware which uses similar email-based C2 channels and hard-coded commands to gain information about the victim's environment; however, IMAPLoader is executed via an injection technique known as 'AppDomain Manager Injection', a technique we have not observed Yellow Liderc using before.

https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/yellow-liderc-ships-its-scripts-delivers-imaploader-malware.html

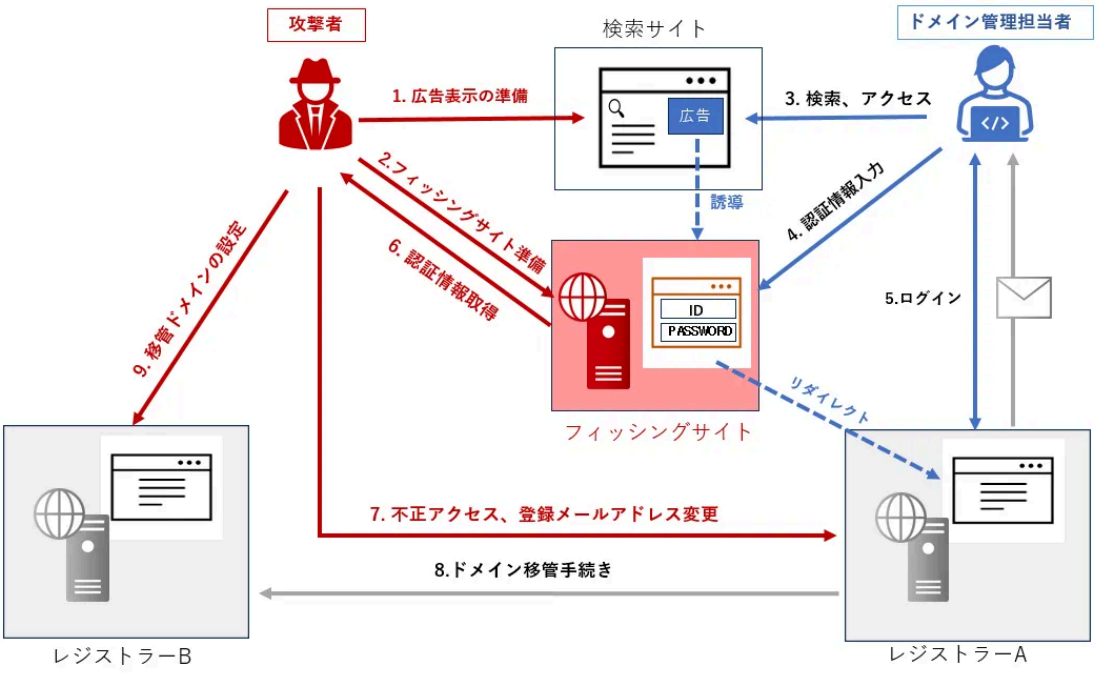
Regional tensions with commodity tradecraft but able to invest in retooling. These regional players are more symptomatic of wider trends.

> - [We] assess with high confidence that YoroTrooper, an espionage-focused threat actor first active in June 2022, likely consists of individuals from Kazakhstan based on their use of Kazakh currency and fluency in Kazakh and Russian. The actor also appears to have a defensive interest in the website of the Kazakhstani state-owned email service and has rarely targeted Kazakh entities.
> - YoroTrooper attempts to obfuscate the origin of their operations, employing various tactics to make its malicious activity appear to emanate from Azerbaijan, such as using VPN exit nodes local to that region.
> - YoroTrooper's targeting appears to be focused on Commonwealth of Independent States (CIS) countries, and the operators have compromised multiple state-owned websites and accounts belonging to government officials of these countries between May and August 2023.
> - Our findings also indicate that, in addition to commodity and custom malware, YoroTrooper continues to rely heavily on phishing emails that direct victims to credential harvesting sites.
> - Recent retooling efforts by YoroTrooper demonstrate a conscious effort to move away from commodity malware and increasingly rely on new custom malware spanning across different platforms such as Python, PowerShell, GoLang and Rust.

https://blog.talosintelligence.com/attributing-yorotrooper/

Reporting out of Japan which highlights the need for focus around DNS domain name security and what happens when it goes wrong.

> a case of domain hijacking in which a domain used in Japan was illegally transferred to another registrar. This time, we will introduce an example of such an attack.
>
> The attacker then used the stolen credentials to log into the registrar's legitimate site and proceed to transfer the domain to another registrar. Furthermore, although the domain administrator was using the domain transfer lock function for the target domain, the attacker himself released the domain transfer lock. In the process of unlocking the domain transfer lock, an email is sent to the contact email address to confirm the user's intention, and the email is used to approve the request, but this email address has also been changed by the attacker.



https://blogs-jpcert-or-jp.translate.goog/ja/2023/10/domain-hijacking.html?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en-US&_x_tr_pto=wapp

First North Korea and now others, the intent here is interesting and something to be aware of. It will be interesting to see how LinkedIn respond given what appears to be an uptick in activity over the platform.

> [We] observed a malicious campaign that employs **LinkedIn** messages as a vector for executing **identity theft attacks**. In this campaign, compromised LinkedIn accounts are utilized to send messages to users with the aim of compromising their accounts by illicitly procuring their cookies, session data, and browser credentials.
>
> The malware employed in these attacks has been positively identified as a member of the **DuckTail** family. This malware variant also possesses an automated functionality, enabling it to execute **Facebook Business hijacking** attacks, thereby providing the attackers with access to the email associated with any potential Facebook Business account owned by the victim.
>
> The observed attacks have targeted professionals belonging to **various Italian companies, especially in the technology sector**. The attackers have shown a preference for focusing on personnel from the sales and finance departments of the targeted companies.

https://blog.cluster25.duskrise.com/2023/10/25/the-duck-is-hiring

Tim Berghoff provides further reporting which hints at the challenges around compromised advertising accounts. We have seen they have been used in cyber operations by a range of actors.

> Criminals hijack business accounts on Facebook and run their own advertising campaigns in someone else's name and at the expense of those affected. This quickly results in thousands of euros in damages for the actual account holders - not to mention the damage to their reputation.

https://www.gdatasoftware.com/blog/2023/10/37814-meta-hijacked-malicious-ads

The takeaway from this reporting is that Gitlab was used for malicious payload hosting.

https://medium.com/walmartglobaltech/icedid-gets-loaded-af073b7b6d39

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

Matthew provides a good end-to-end walkthrough on how to recover the payload and analyse it using a variety of tools. More who learn this, the more we automate and more cost we can impose.

> I will demonstrate a process for decoding a simple .hta loader used to load cobalt strike shellcode. We will perform initial analysis using a text editor, and use CyberChef to extract embedded shellcode. From here we will validate the shellcode using an emulator (SpeakEasy) and perform some basic analysis using Ghidra.

https://embee-research.ghost.io/malware-analysis-decoding-a-simple-hta-loader/

Jiacen Xu, **Xiaokui Shu** and **Zhou Li** bring some science to the application of machine learning in detection. This type of evidenced based work is very important as we wrestle with various claims of efficacy.

> Graph security analytics (GSA) that can model the complex communication patterns between users/hosts/processes have been extensively developed and deployed. Among the techniques that power GSAs, Unsupervised Network Representation Learning (UNRL) is gaining traction, which learns a latent graph representation, i.e., node embedding, and customizes it for different downstream tasks. Prominent advantages have been demonstrated by UNRL-based GSAs, as UNRL trains a detection model in an unsupervised way and exempts the model developers from the duty of feature engineering. In this paper, we revisit the designs of previous UNRL-based GSAs to understand how they perform in real-world settings. We found their performance is questionable on large-scale, noisy log datasets like LANL authentication dataset, and the main reason is that they follow the standard UNRL framework that trains a generic model in an attack-agnostic way. We argue that generic attack characteristics should be considered, and propose Argus, a UNRL-based GSA with new encoder and decoder designs. Argus is also designed to work on discrete temporal graphs (DTG) to exploit the graph temporal dynamics. Our evaluation of two large-scale datasets, LANL and OpTC, shows it can outperform the state-of-the-art approaches by a large margin.

https://www.computer.org/csdl/proceedings-article/sp/2024/313000a012/1RjE9Q5gQrm

How we proactively defend our environments.

7-layer zero trust solution from China which provides an interesting insight to interpretation and adoption of the concept.

> In order to improve the robustness of the intranet and simplify complex internal port policies, Baidu has launched the exploration of zero-trust architecture in recent years, and recently completed the implementation of zero-trust on the 7th layer of the office network. Implementing a zero-trust gateway will usually encounter several key issues. For example, in terms of technical solutions, it is necessary to ensure the stability of the gateway and delay in response to requests; in terms of operational solutions, it is necessary to design a grayscale process to solve the resistance from the business line and the business relationship. line to build trust and more.

https://mp-weixin-qq-com.translate.goog/s/5utSjmXrh5enrAvJmJLFvQ?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=wapp

Defensive advice from the French Government in the guide of ANSSI - Tres Bon!

> ANSSI regularly notes that compromises of information systems (IS) based on an Active Directory (AD) result from the application of poor administration practices and insufficient partitioning. These compromises often start with attacks that target workstations. The attackers then exploit weaknesses in the IS to carry out so-called lateral

> movements and gradually increase their privileges until they obtain total control of the AD. At this level of control of the AD, an attacker is able to set up back doors which provide him with persistent control of the IS, that is to say also of the organization's business processes and data.

https://cyber-gouv-fr.translate.goog/publications/recommandations-pour-ladministration-securisee-des-si-reposant-sur-ad?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en-US&_x_tr_pto=wapp

https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html

Jared Atkinson walks us through an every growing training serious on practical detection engineering - it really is a rich source of learnings.

> In this article, I hope to demonstrate how the operational layer IS the appropriate layer of analysis for those interested in creating behavioral detection analytics.
>
> > ***Note:*** *In this context, a behavioral detection analytic is one that focuses on what the malware does instead of what the malware is. It decouples the action from the actor. This is not to say that detecting known bad malware based on what it is, is a bad idea; we simply are attempting to take the next logical step.*

https://posts.specterops.io/on-detection-tactical-to-functional-f37c9b0b8874

Chrome as Apple has with Private Relay is starting to experiment with IP address protection. Matter of when and not if.

> - **IP Protection will be opt-in initially**. This will help ensure that there is user control over privacy decisions and that Google can monitor behaviors at lower volumes.
> - **It will roll out in a phased manner. Like all of our privacy proposals, we want to ensure that we learn as we go and we recognize that there may also be regional considerations to evaluate.**
> - **We are using a list based approach and only domains on the list in a third-party context will be impacted**. We are conscious that these proposals may cause undesired disruptions for legitimate use cases and so we are just focused on the scripts and domains that are considered to be tracking users.

https://groups.google.com/a/chromium.org/g/blink-dev/c/9s8ojrooa_Q?pli=1

MISP to the rescue

First it was reported there was a dip in the number of implants. Turns out the threat actor upgraded their implant to evade the detection techniques. We can take from this that threat actors read public reporting. This also shows the value of good threat research..

> Investigated network traffic to a compromised device has shown that the threat actor has upgraded the implant to do an extra header check. Thus, for a lot of devices, the implant is still active, but now only responds if the correct `Authorization` HTTP header is set.

https://github.com/fox-it/cisco-ios-xe-implant-detection

Olaf Hartong gives the world a massive powerup with this capability. This is quality defensive research and engineering incarnate.

> FalconHound is a blue team multi-tool. It allows you to utilize and enhance the power of BloodHound in a more automated fashion. It is designed to be used in conjunction with a SIEM or other log aggregation tool.
>
> One of the hardest releationships to gather for BloodHound is the local group memberships and the session information. As blue teamers we have this information readily available in our logs. FalconHound can be used to gather this information and add it to the graph, allowing it to be used by BloodHound.
>
> This is just an example of how FalconHound can be used. It can be used to gather any information that you have in your logs or security tools and add it to the BloodHound graph.

https://github.com/FalconForceTeam/FalconHound

How they got in and what they did.

This is a rather interesting breach involving the support portal and then data uploaded to that portal enabling breaches of clients. The clients impacted are the ones who detected it. All the report follows, but lots of lessons learnt here.

> Okta Security has identified adversarial activity that leveraged access to a stolen credential to access Okta's support case management system.

https://sec.okta.com/harfiles

> - October 2, 2023 – Detected and remediated identity centric attack on an in-house Okta administrator account and alerted Okta
> - October 3, 2023 – Asked Okta support to escalate to Okta security team given initial forensics pointing to a compromise within Okta support organization
> - October 11, 2023 and October 13, 2023 – Held Zoom sessions with Okta security team to explain why we believed they might be compromised
> - October 19, 2023 – Okta security leadership confirmed they had an internal breach, and BeyondTrust was one of their affected customers.

https://www.beyondtrust.com/blog/entry/okta-support-unit-breach

> On Wednesday, October 18, 2023, we discovered attacks on our system that we were able to trace back to Okta – threat actors were able to leverage an authentication token compromised at Okta to pivot into Cloudflare's Okta instance.

https://blog.cloudflare.com/how-cloudflare-mitigated-yet-another-okta-compromise/

> We detected suspicious activity on our Okta instance related to their Support System incident. After a thorough investigation, we concluded that no 1Password user data was accessed

https://blog.1password.com/okta-incident/

Our attack surface.

Non-admin arbitrary memory read/write is possible and one to add to the list.

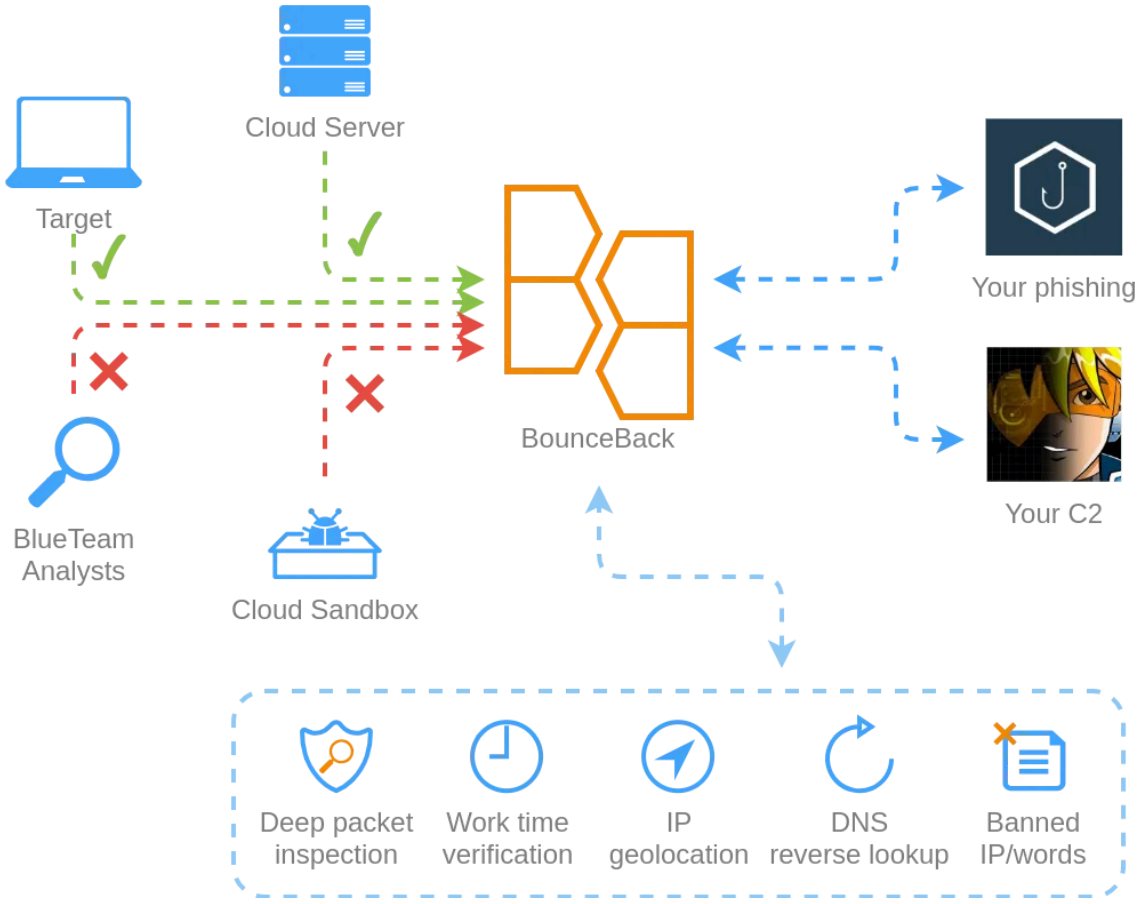
> An improper privilege management in the AMD Radeon™ Graphics driver may allow an authenticated attacker to craft an IOCTL request to gain I/O control over arbitrary hardware ports or physical addresses resulting in a potential arbitrary code execution.

https://www.amd.com/en/resources/product-security/bulletin/amd-sb-6009.html

Attack capability, techniques and trade-craft.

Offensive use by threat actors in 3..2..

> BounceBack is a powerful, highly customizable and configurable reverse proxy with WAF functionality for hiding your C2/phishing/etc infrastructure from blue teams, sandboxes, scanners, etc. It uses real-time traffic analysis through various filters and their combinations to hide your tools from illegitimate visitors.
>
> The tool is distributed with preconfigured lists of blocked words, blocked and allowed IP addresses.



https://github.com/D00Movenok/BounceBack

Beau Bullock & **Steve Borosh** show attackers really do think in graphs and the value of doing so..

> We built a post-compromise toolset called **GraphRunner** for interacting with the Microsoft Graph API. It provides various tools for performing reconnaissance, persistence, and pillaging of data from a Microsoft Entra ID (Azure AD) account. Below are some of the main features. At the end of the blog post, make sure to take a peek at the potential attack path scenarios we have laid out. There are a few in there we think may be quite interesting to both offensive and defensive security team members.

https://www.blackhillsinfosec.com/introducing-graphrunner/

Elliot Killick refines this known techniques which we can expect to see adopted by the various post compromise frameworks and others.

> While mostly being a decisive technique, DLL hijacking has always had one **huge** disadvantage in the way that it executes our third-party code once loaded into the process. It's known as **Loader Lock**, and when our third-party code is run, it's subject to all its strict limitations. These include creating processes, doing network I/O, calling registry functions, creating graphical windows, loading additional libraries, and much more. Trying to do any of these things under Loader Lock will likely **crash or hang** the application.
>
> [We] cleanly workaround Loader Lock but, in the end, disable it outright. Plus, coming up with some stable mitigation & detection mechanisms defenders can use to help guard against DLL hijacking.

https://elliotonsecurity.com/perfect-dll-hijacking/

> Our latest post in the SaaS attacks matrix series is focused on external phishing via Slack. Unlike email, IM apps and the messages within them are typically more trusted by employees, making social engineering via Slack a juicy target.

https://pushsecurity.com/blog/slack-phishing-for-initial-access/

What is being exploited.

Further insight which has led to over 10,000 routers being compromised. The lesson here is that actors read intel reporting and will in some situations respond as they did here by updating their implants to evade.

> The attacker first exploited CVE-2023-20198 to gain initial access and issued a privilege 15 command to create a local user and password combination. This allowed the user to log in with normal user access.
>
> The attacker then exploited another component of the web UI feature, leveraging the new local user to elevate privilege to *root* and write the implant to the file system. Cisco has assigned CVE-2023-20273 to this issue.
>
> - **CVE-2023-20198** has been assigned a CVSS Score of 10.0.
> - **CVE-2023-20273** has been assigned a CVSS Score of 7.2.

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

NCSC put out a UK specific alert '**xploitation of Cisco IOS XE vulnerabilities affecting UK organisations:**

https://www.ncsc.gov.uk/news/cisco-ios-xe-vulnerabilities

When you can leak session cookies authentication can be bypassed so this is a serious vulnerability which we know is now being actively scanned for.

> We could clearly see a lot of leaked memory immediately following the JSON payload. While a lot of it was null bytes, there was some suspicious looking information in the response.

https://www.assetnote.io/resources/research/citrix-bleed-leaking-session-tokens-with-cve-2023-4966

https://github.com/assetnote/exploits/tree/main/citrix/CVE-2023-4966

First reported as being exploited by China, now exploitable by all threat actors..

> This module exploits an improper input validation issue in Atlassian Confluence, allowing arbitrary HTTP parameters to be translated into getter/setter sequences via the XWorks2 middleware and in turn allows for Java objects to be modified at run time. The exploit will create a new administrator user and upload a malicious plugins to get arbitrary code execution. All versions of Confluence between 8.0.0 through to 8.3.2, 8.4.0 through to 8.4.2, and 8.5.0 through to 8.5.1 are affected.

https://github.com/rapid7/metasploit-framework/pull/18461

Dylan Evans shows an example of Intelligent Platform Management Interface exploitation here. IPMI is important as it includes KVM over IP, remote virtual media and out-of-band embedded web-server interface functionality etc. The worry is also it also won't be protected by EDR etc.

> This tool exploits the vulnerability detailed in CVE-2013-4786, which allows unauthorized users to retrieve salted password hashes from IPMI devices via the RAKP (Remote Authentication Key Protocol) mechanism. This is

> achieved by initiating an IPMI 2.0 RAKP authentication process with a cipher suite that enables 'None' authentication, allowing the retrieval of salted password hashes

https://github.com/fin3ss3g0d/CosmicRakp

Low level tooling and techniques for attack and defence researchers…

Excellent work here to extend Yara to support powerful memory scanning.

> allows Yara rules to query memory protection for live process memory. This allows writing conditions like for any i in (1..#a) : (memory.Protection(@a[i]) & memory.EXECUTE == memory.EXECUTE) for strings that should only match on executable memory.

https://github.com/VirusTotal/yara/pull/1991

This is an exciting analysis framework which should accelerate some analysis techniques.

> SHAREM is intended to be the ultimate Windows shellcode tool, with support to emulate over 20,000 WinAPIs, virtually all user-mode Windows syscalls, and SHAREM provides numerous new features. SHAREM was released on September 29, 2022. SHAREM contains an emulator, a disassembler, timeless debugging, brute-force deobfuscation, and many other features. SHAREM's emulator can also display complete structures (or even structures within structures) and it can allow encoded shellcode to deobfuscate itself. SHAREM logs output from all WinAPIs and Windows syscalls analyzed, and it also breaks each into many categories and subcategories. SHAREM's complete code coverage also allows it to discover unreachable functionality.

https://github.com/Bw3ll/sharem

Impressive project with material utility for malware analysts.

> Run Mac OS X in Docker with near-native performance! X11 Forwarding! iMessage security research! iPhone USB working! macOS in a Docker container!
>
> Conduct Security Research on macOS using both Linux & Windows!

https://github.com/sickcodes/Docker-OSX

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

- Aggregate reporting
    - macOS Malware 2023
- Common Abuses on Mastodon: A Primer
- Scaling up prime factorization with self-organizing gates: A memcomputing approach
- Hack.lu 2023: Introduction To Cyberwarfare: Theory And Practice
- Artificial intelligence
    - Beyond Memorization: Violating Privacy Via Inference with Large Language Models
    - nbdefense: Secure Jupyter Notebooks and Experimentation Environment
    - modelscan: Protection against Model Serialization Attacks

    - rebuff: LLM Prompt Injection Detector
- Books
    - *None this week*
- Events
    - HITB2023HKT - Main Track videos
    - The BlueHat Podcast: BlueHat Oct 23 Day 1 Keynote: John Lambert

Finally on the video front this week The British Hacker That Joined ISIS
