PRACTICAL ADVERSARY INTELLIGENCE

WILLIAM THOMAS
CYBER THREAT INTELLIGENCE RESEARCHER
EQUINIX THREAT ANALYSIS CENTER (ETAC)™

TALK CONTENTS

How to extract useful information about Threat Actor Groups and Attack Campaigns

Identify sources of Adversary Intelligence

Leveraging Free OSINT Tools

Building a Threat Actor Database

WHAT'S THE POINT OF CTI?

- Defend and mitigate sophisticated attacks
- Detect and remediate compromised systems
- Impose cost and deter adversaries
- Protect others through intelligence sharing
- Fulfil Priority Intelligence Requirements

STOP HIM

INTELLIGENCE GATHERING

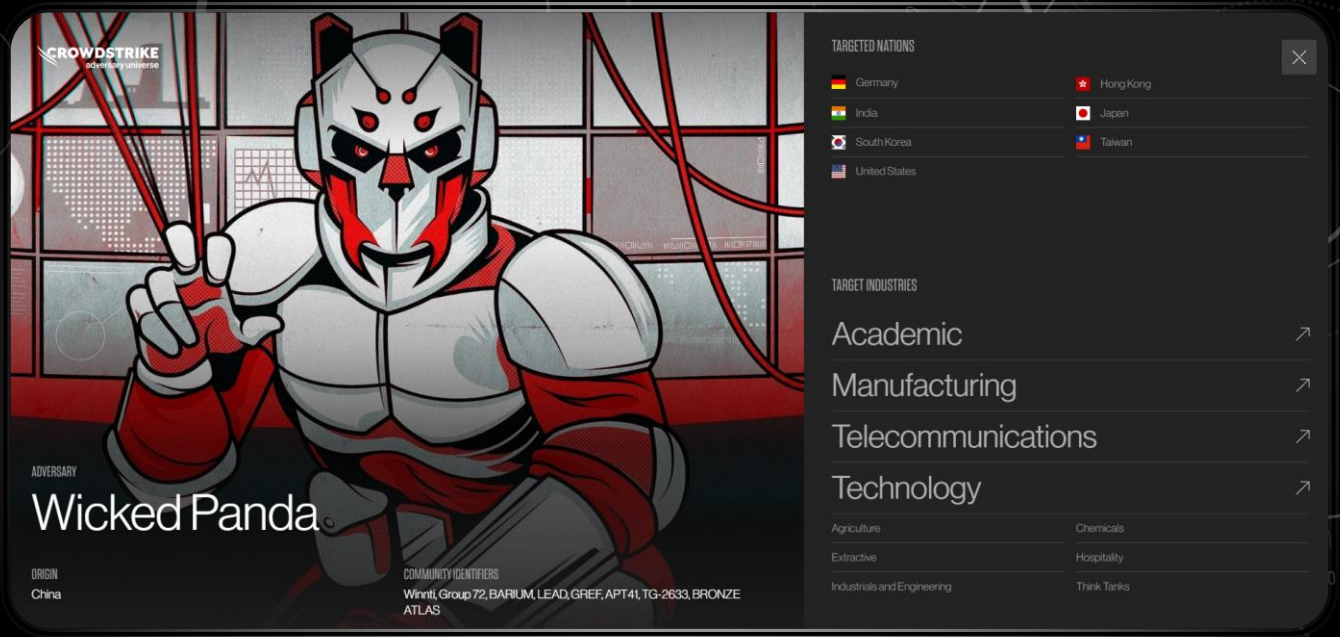
- Priority Intelligence Requirements (PIRs)
- Requests for Information (RFIs)
- Objectives and Key Results (OKRs)
- Identification of Adversaries
- Sector-specific Threats

ATTRIBUTION MATTERS

- Advanced Persistent Threats (APTs)
- Organised Cybercriminals (e.g. Ransomware)
- Other (e.g. Hacktivists, Mercenaries, Unknowns)
- State-sponsored or State-apathetic?
- Based on Vendor Telemetry

THREAT ACTOR PROFILES

- Tools, Software, Infrastructure
- Tactics, Techniques, and Procedures
- Indicators of Compromise
- Attribution



Secureworks

CHINA

BRONZE ATLAS

Objectives	Espionage
Aliases	APT41 (FireEye), Axiom, BARIUM (Microsoft), Blackfly (Symantec), GREF, Group 72 (Talos), Red Kelpie (PWC), TG-2633 (SCWX CTU), Wicked Panda (CrowdStrike), Winnti
Tools	Acehash, CCleaner v5.33 backdoor, China Chopper, Dicey MSDN, HUC Proxy Malware (Htran), Mimikatz, PlugX, PowerShell Empire, RbDoor, Speculoos, Winnti

BRONZE ATLAS has been operating since at least 2007. CTU researchers assess with high confidence that the group's intent is towards theft of intellectual property from organizations in developed economies, and with moderate confidence that this is on behalf of China to support decision making in a range of Chinese economic sectors. The group primarily use scan-and-exploit and phishing for initial access and enable their intrusions through theft of code signing certificates from technology and gaming organizations. CTU researchers have linked BRONZE ATLAS to targeted attacks on organizations in the pharmaceuticals, media, human rights, fossil fuels and agriculture sectors. The group has also been publicly linked to the high collateral supply chain compromises leveraging software updates for Ccleaner and Netsarang to compromise users in 2017. BRONZE ATLAS is also known as APT41, Axiom or Winnti in public reporting.

MITRE | ATT&CK

Home > Groups > APT41

APT41

APT41 is a threat group that researchers have assessed as Chinese state-sponsored espionage group that also conducts financially-motivated operations. Active since at least 2012, APT41 has been observed targeting healthcare, telecom, technology, and video game industries in 14 countries. APT41 overlaps at least partially with public reporting on groups including BARIUM and Winnti Group.[1][2]

ID: G0096
Associated Groups: WICKED PANDA
Contributors: Kyaw Pyiyt Htet, @KyawPyiytHtet
Version: 3.0
Created: 23 September 2019
Last Modified: 15 October 2021

Version Permalink

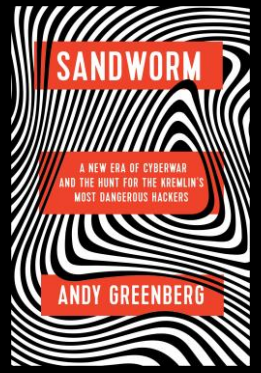
Associated Group Descriptions

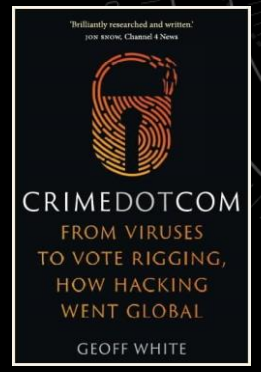
Name	Description
WICKED PANDA	[3]

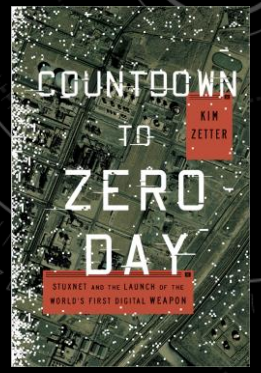
OSINT RESEARCH

RESEARCHER HOTSPOTS

BOOKS



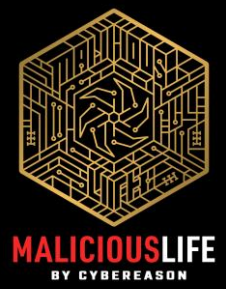




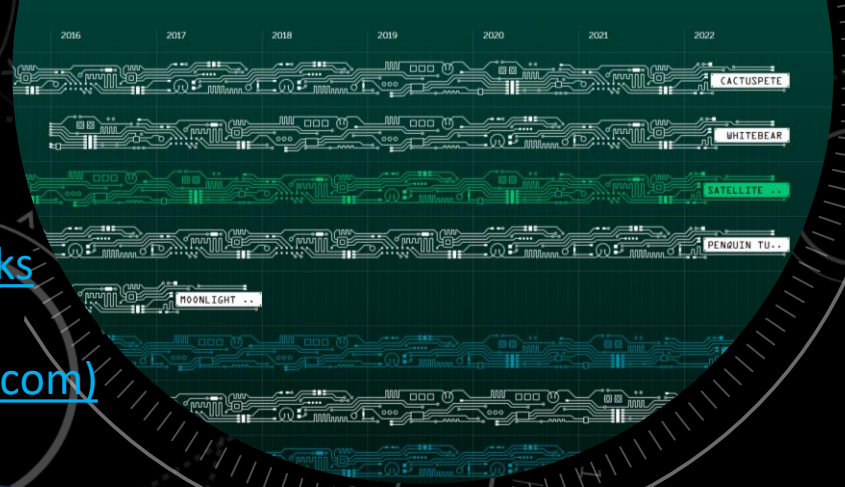
CONVERSATIONS

CONFERENCES

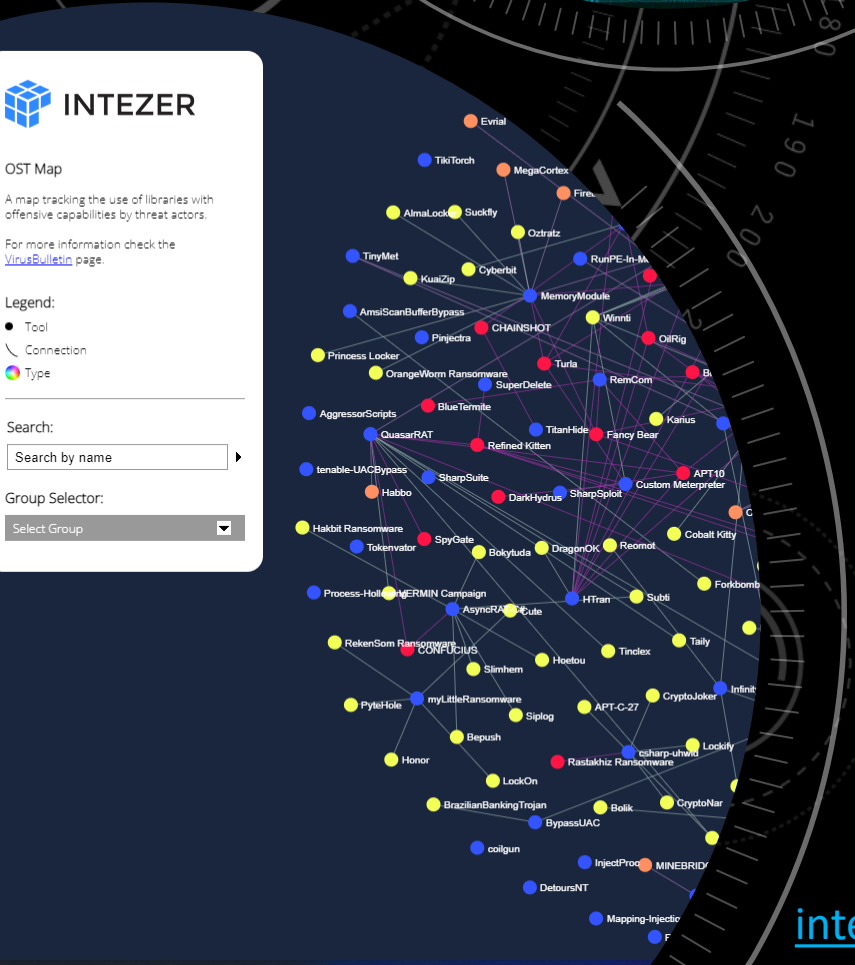
PODCASTS



APT DATABASES



[Targeted cyberattacks logbook (securelist.com)](https://securelist.com/)



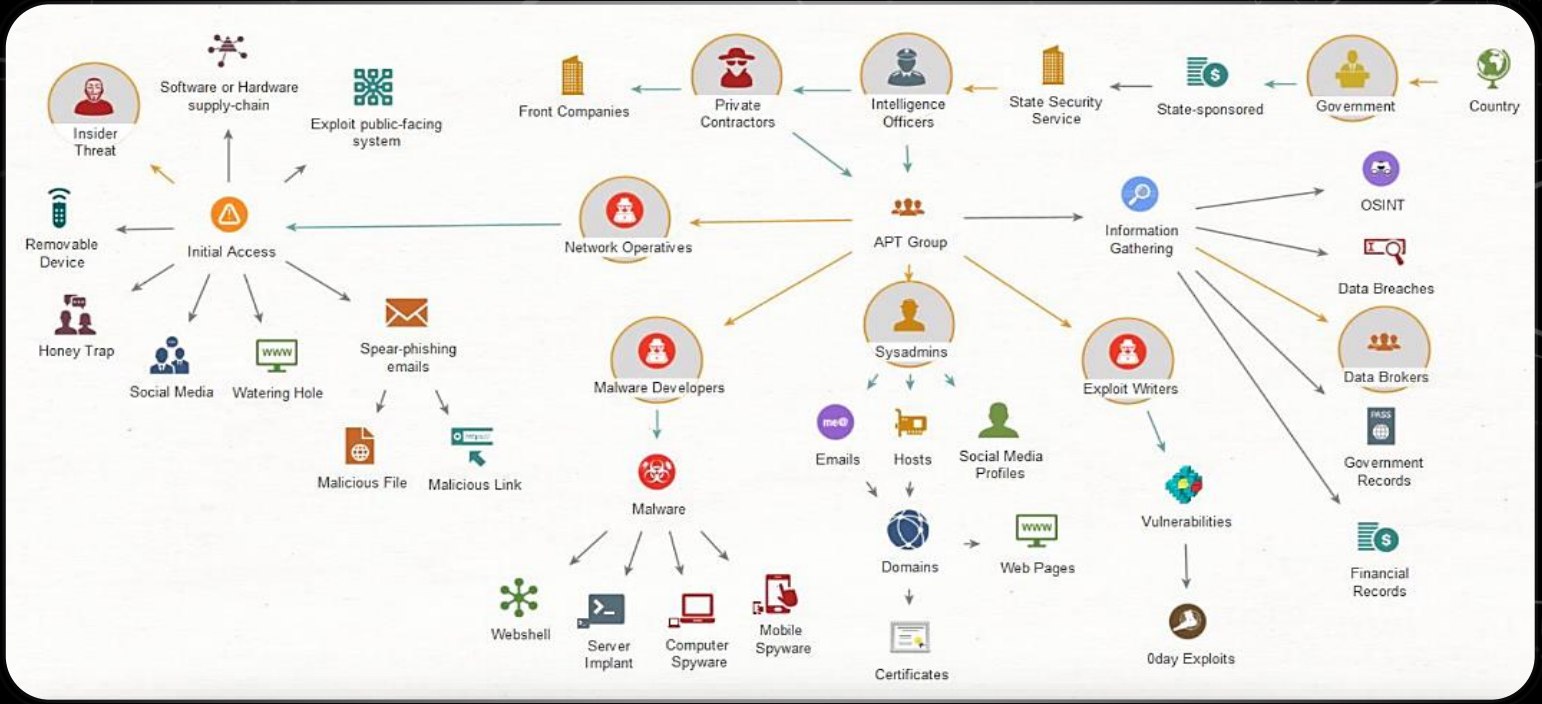
intezer.com/ost-map/

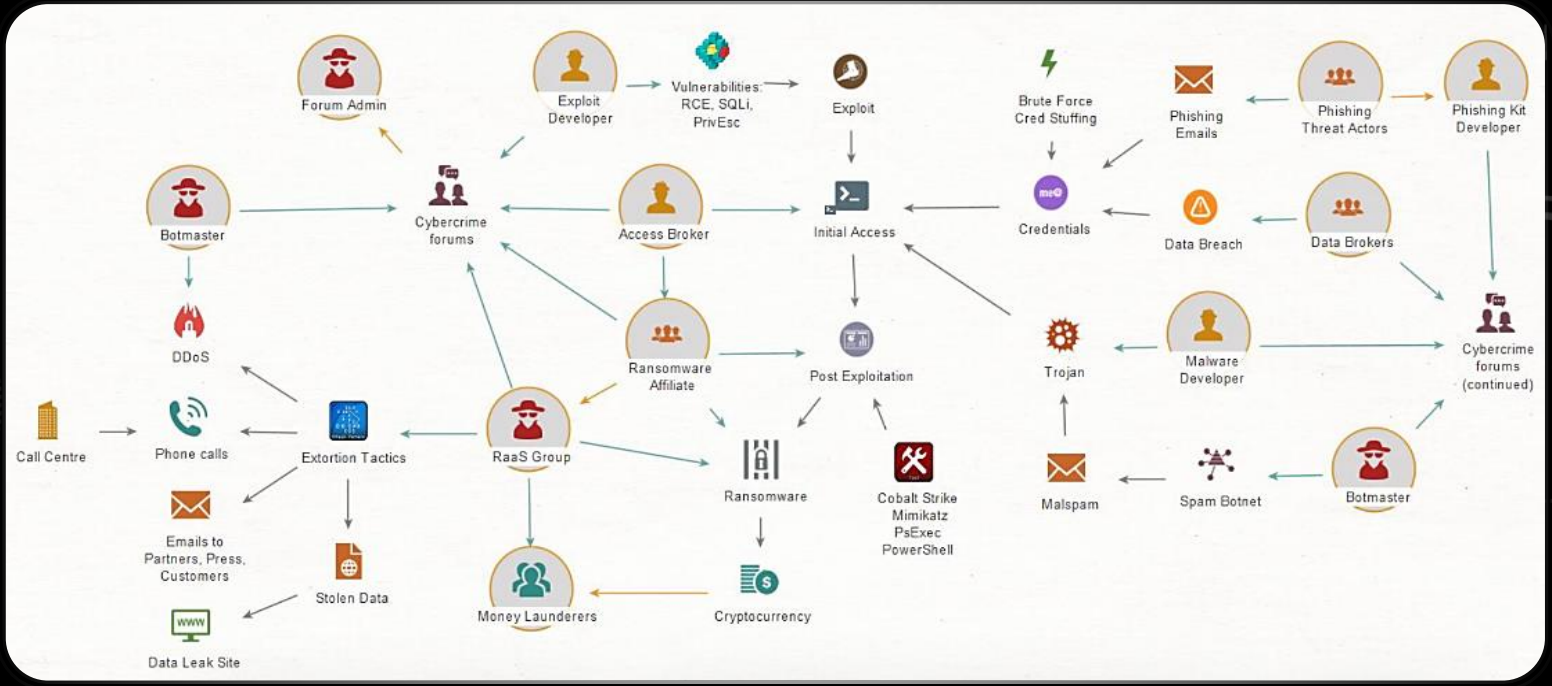
ti.qianxin.com/apt/

[andreacristaldi.github.io/APTmap/](https.://andreacristaldi.github.io/APTmap/)

[Open-source-tools-for-CTI/Adversary Intelligence.md at master · BushidoUK/Open-source-tools-for-CTI (github.com)](https://github.com/BushidoUK/Open-source-tools-for-CTI/Adversary Intelligence.md)

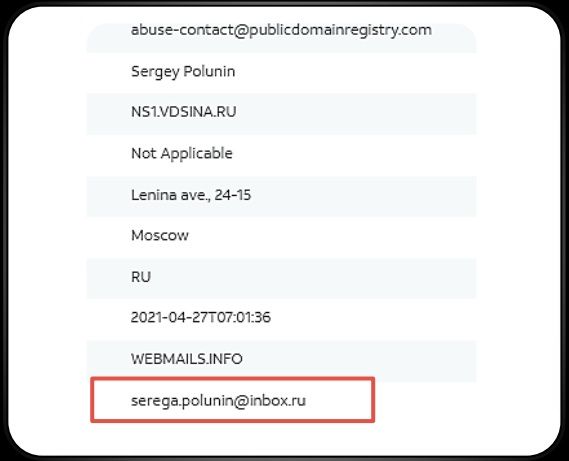
MALTEGO ENTITY RELATIONSHIP ANALYSIS



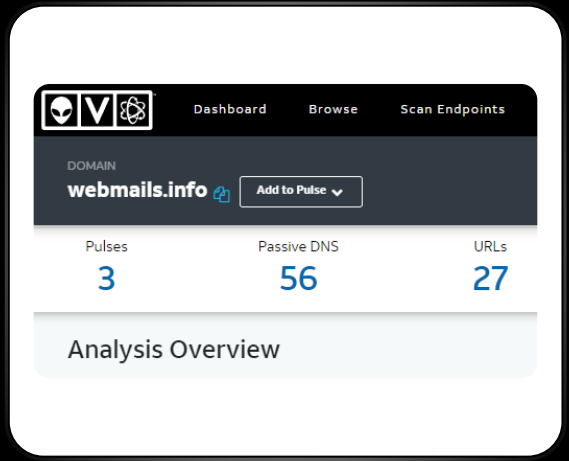


STATE CRIME

IOCS AND OTX ALIENVAULT



abuse-contact@publicdomainregistry.com	
Sergey Polunin	
NS1.VDSINA.RU	
Not Applicable	
Lenina ave., 24-15	
Moscow	
RU	
2021-04-27T07:01:36	
WEBMAILS.INFO	
serega.polunin@inbox.ru	



e.mail.ru.inbox.webmails.info	A	62.113.113.38	2021-08-09 10:55
e.mail.ru.webmails.info	A	62.113.113.38	2021-08-14 10:57
email.mfa.gov.ge.webmails.info	A	109.234.36.65	2021-09-16 06:44
email.mfa.gov.ge.webmails.info	A	62.113.113.38	2021-06-22 10:56
mail.agro.uz.webmails.info	A	109.234.36.65	2021-09-16 06:44
mail.economy.ge.webmails.info	A	109.234.36.65	2021-09-16 06:44
mail.mfa.am.webmails.info	A	109.234.36.65	2021-09-16 06:44
mail.mfa.gov.kg.webmails.info	A	109.234.36.65	2021-09-16 06:44
mail.mfa.uz.webmails.info	A	109.234.36.65	2021-09-16 06:44
mail.mift.uz.webmails.info	A	109.234.36.65	2021-09-16 06:44
scoring.mra.gov.ge.webmails.info	A	109.234.36.65	2021-09-16 06:44
scoring.mra.gov.ge.webmails.info	A	62.113.113.38	2021-08-11 05:56

- Related Pulses
- IOC validation
- Connected samples
- Passive DNS

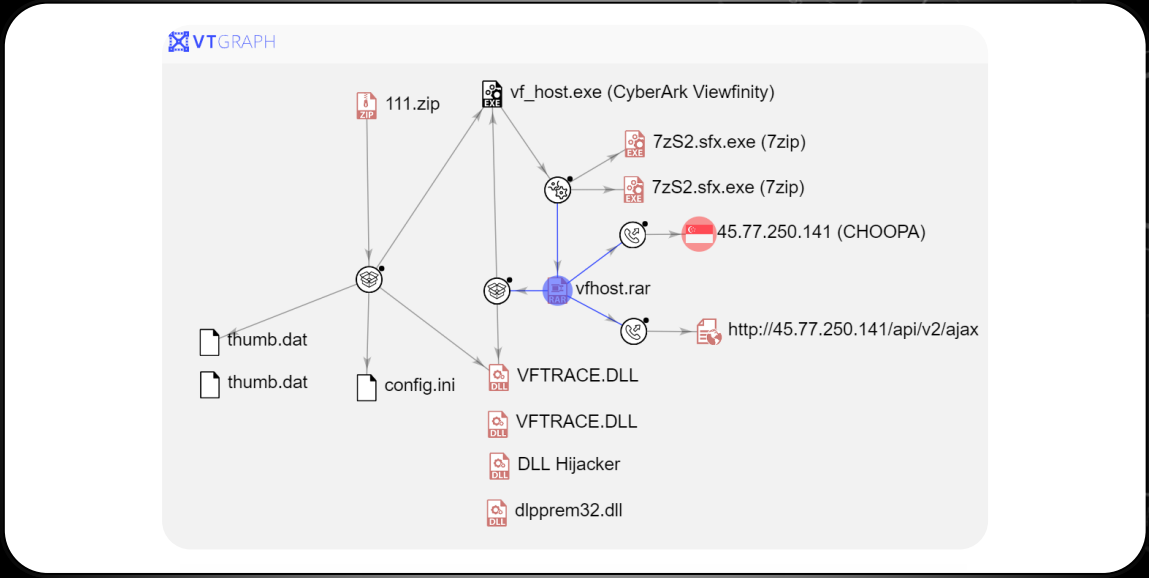
EMEA and APAC governments targeted in widespread credential harvesting campaign ⋆ Cyjax

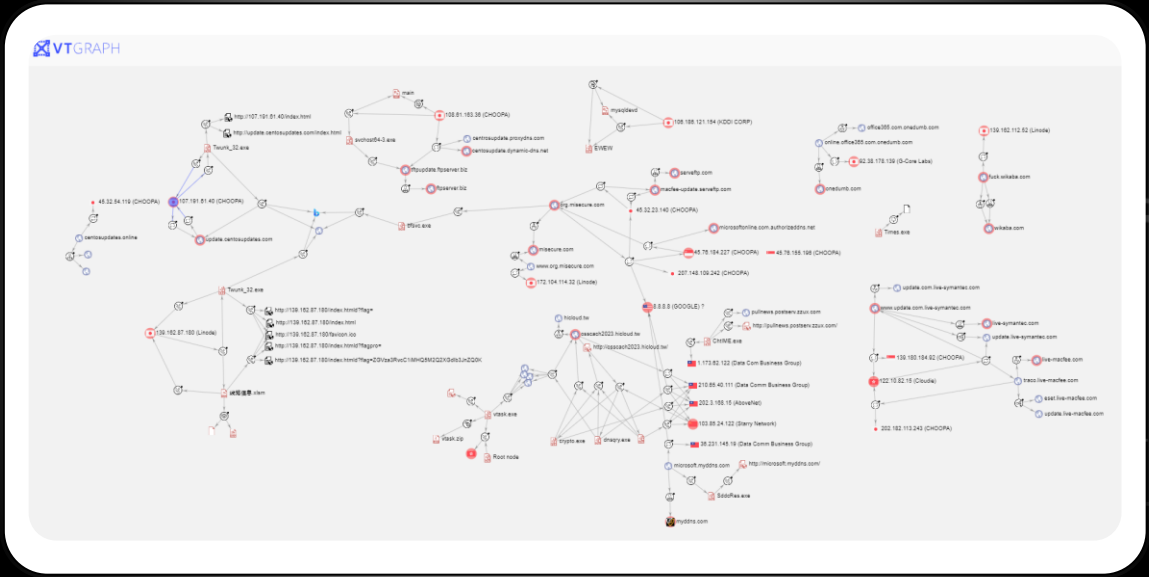
Domain: webmails.info - AlienVault - Open Threat Exchange

VIRUSTOTAL AND VT GRAPH

- [BushidoUK/Exploring-APT-campaigns: Further investigation in to APT campaigns disclosed by private security firms and security agencies (github.com)]

IRONTIGER (APT27, LUCKYMOUSE)

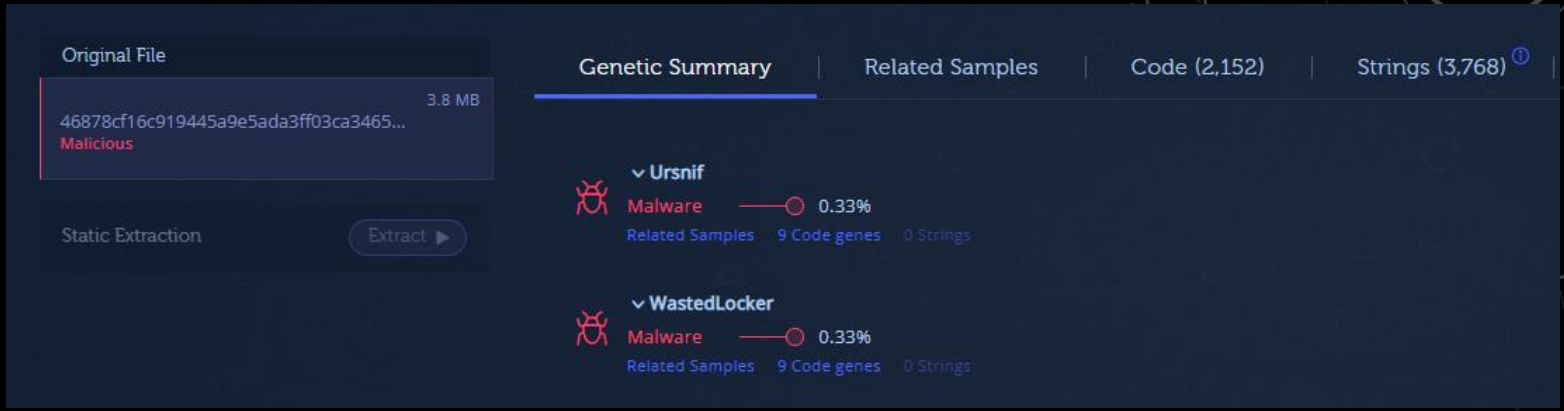




BLACKTECH (CIRCUIT PANDA)

GENETIC ANALYSIS OF CODE

```
============================
    __,---.
   /__|o\  )
    `-\ / /   MACAW
      ,) (,   LOCKER
     //   \\
    {(     )}
=======""===""==============
Data in your network has been stolen and encrypted.
```



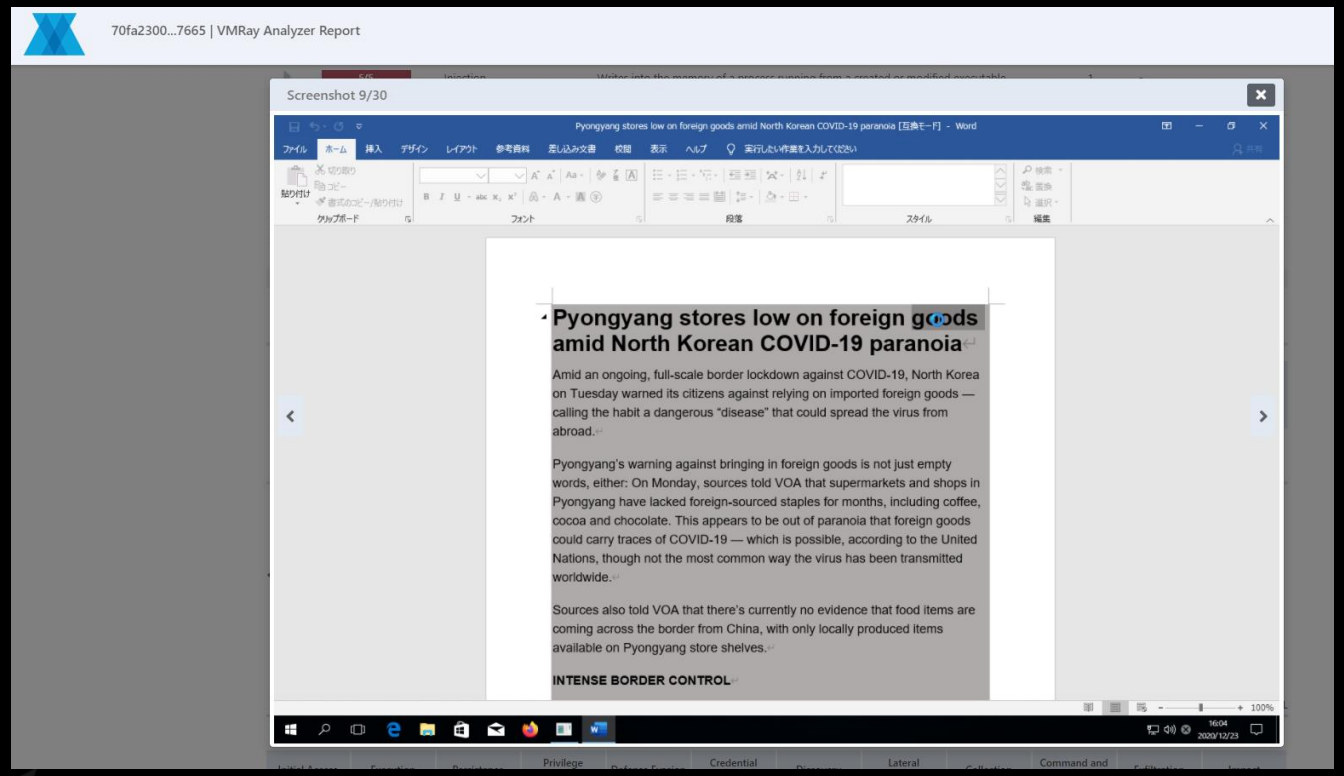
[Malicious b9ee938be15921b1a372bd97372a9c31 - Intezer]

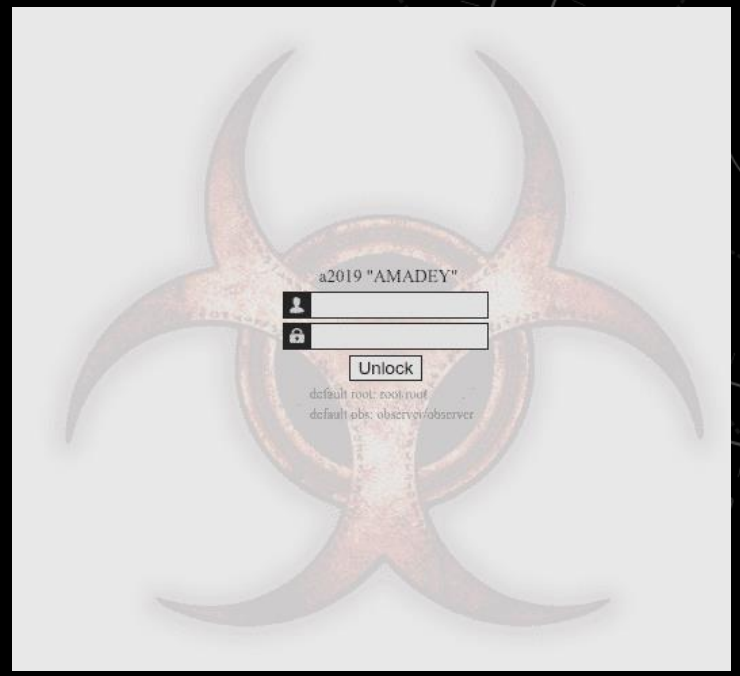
Alibaba	Ransom:Win32/Wasted.19e9bc74	ALYac	Trojan.Ransom.MacawLocker
ESET-NOD32	A Variant Of Win32/Packed.VMProtect.ZF	FireEye	Generic.mg.b9ee938be15921b1
Jiangmin	Trojan.Wasted.b	K7AntiVirus	Riskware (0040eff71)
K7GW	Riskware (0040eff71)	Kaspersky	Trojan-Ransom.Win32.Wasted.af
McAfee-GW-Edition	BehavesLike.Win32.Backdoor.wc	Microsoft	Ransom:Win32/Macaw.STA

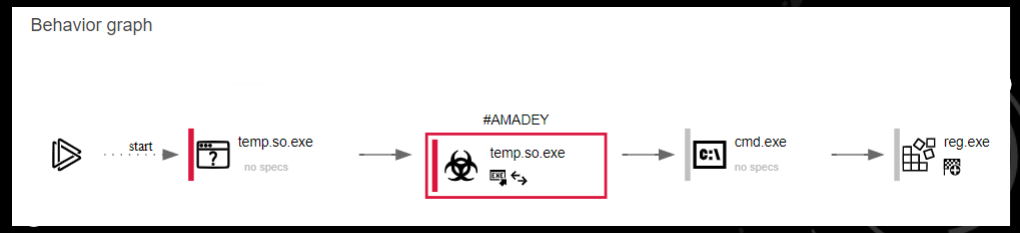
[VirusTotal - File - 46878cf16c919445a9e5ada3ff03ca3465c03323a3e8b31c2de38eae1c9259e4]

PUBLIC SANDBOXES

[70fa2300...7665 | VMRay Analyzer Report]







[Amadey Trojan distributed by DPRK-affiliated APT groups (bushidotoken.net)]

- VMRay, JoeSandbox, Hybrid-Analysis, Any.Run

MITRE | ATT&CK®

TeamTNT

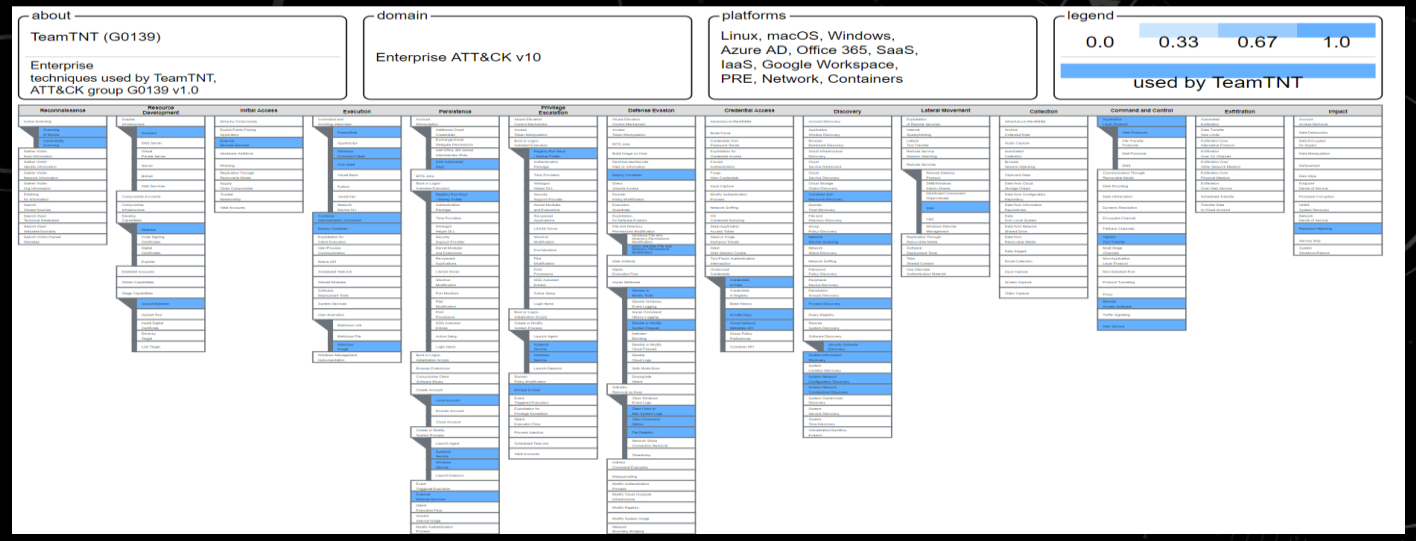
ID: G0139

Contributors: Will Thomas, Cyjax

Version: 1.0

Created: 01 October 2021

Last Modified: 15 October 2021

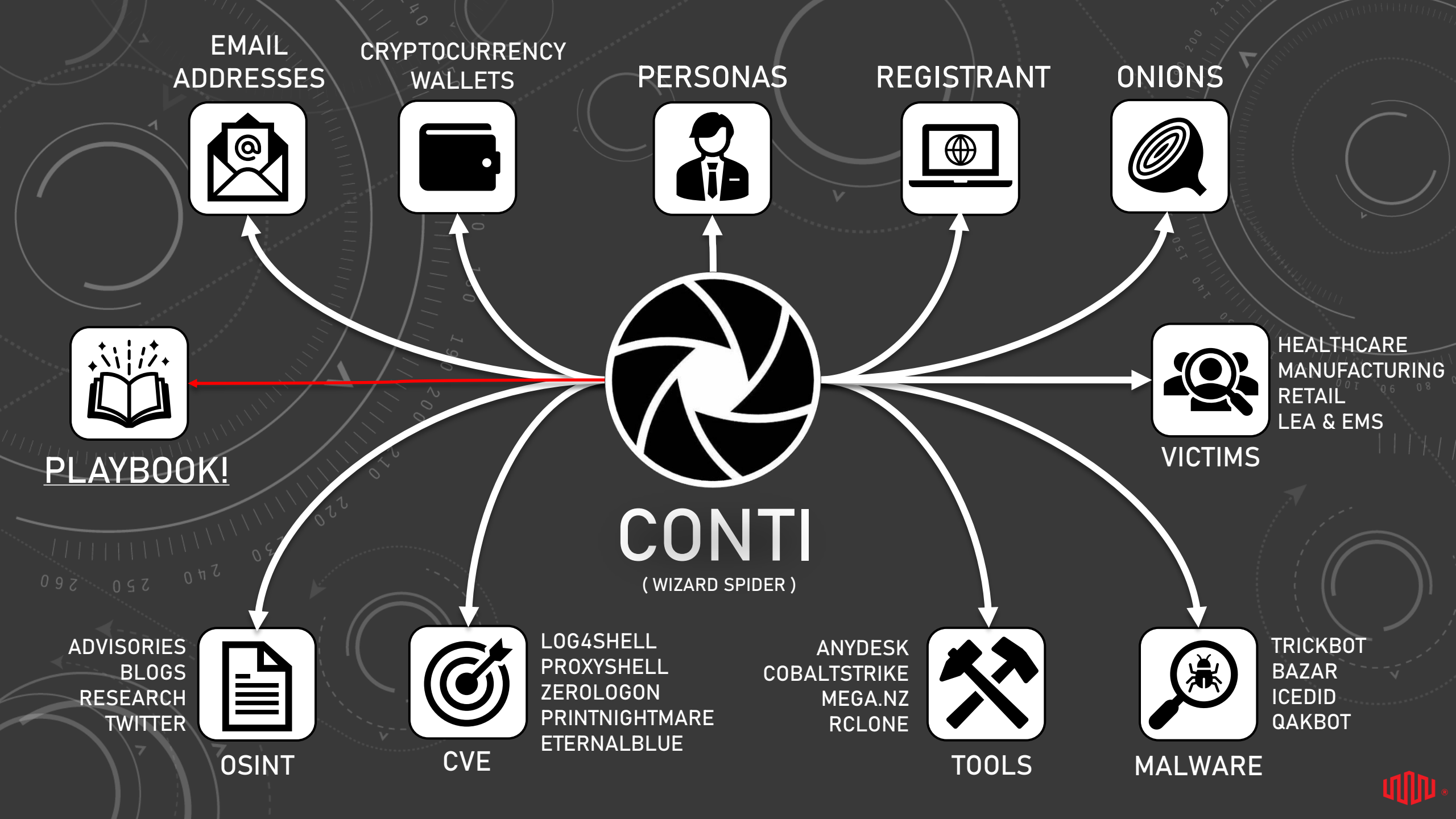


References

1. Quist, N. (2020, October 5). Black-T: New Cryptojacking Variant from TeamTNT. Retrieved September 22, 2021.
2. Stroud, J. (2021, May 25). Taking TeamTNT's Docker Images Offline. Retrieved September 22, 2021.
3. Fishbein, N. (2020, September 8). Attackers Abusing Legitimate Cloud Monitoring Tools to Conduct Cyber Attacks. Retrieved September 22, 2021.
4. Cado Security. (2020, August 16). Team TNT – The First Crypto-Mining Worm to Steal AWS Credentials. Retrieved September 22, 2021.
5. Chen, J. et al. (2021, February 3). Hildegard: New TeamTNT Cryptojacking Malware Targeting Kubernetes. Retrieved April 5, 2021.
6. Fiser, D. Oliveira, A. (n.d.). Tracking the Activities of TeamTNT A Closer Look at a Cloud-Focused Malicious Actor Group. Retrieved September 22, 2021.
7. AT&T Alien Labs. (2021, September 8). TeamTNT with new campaign aka Chimaera. Retrieved September 22, 2021.
8. Kol, Roi. Morag, A. (2020, August 25). Deep Analysis of TeamTNT Techniques Using Container Images to Attack. Retrieved September 22, 2021.
9. Intezer. (2021, September 1). TeamTNT Cryptomining Explosion. Retrieved October 15, 2021.

TACTICS, TECHNIQUES, AND PROCEDURES

TEAMTNT, GROUP G0139 | MITRE ATT&CK®


EMAIL ADDRESSES
CRYPTOCURRENCY WALLETS
PERSONAS
REGISTRANT
ONIONS
PLAYBOOK!
HEALTHCARE
MANUFACTURING
RETAIL
LEA & EMS
VICTIMS
CONTI
(WIZARD SPIDER)
ADVISORIES
BLOGS
RESEARCH
TWITTER
OSINT
LOG4SHELL
PROXYSHELL
ZEROLOGON
PRINTNIGHTMARE
ETERNALBLUE
CVE
ANYDESK
COBALTSTRIKE
MEGA.NZ
RCLONE
TOOLS
TRICKBOT
BAZAR
ICEDID
QAKBOT
MALWARE

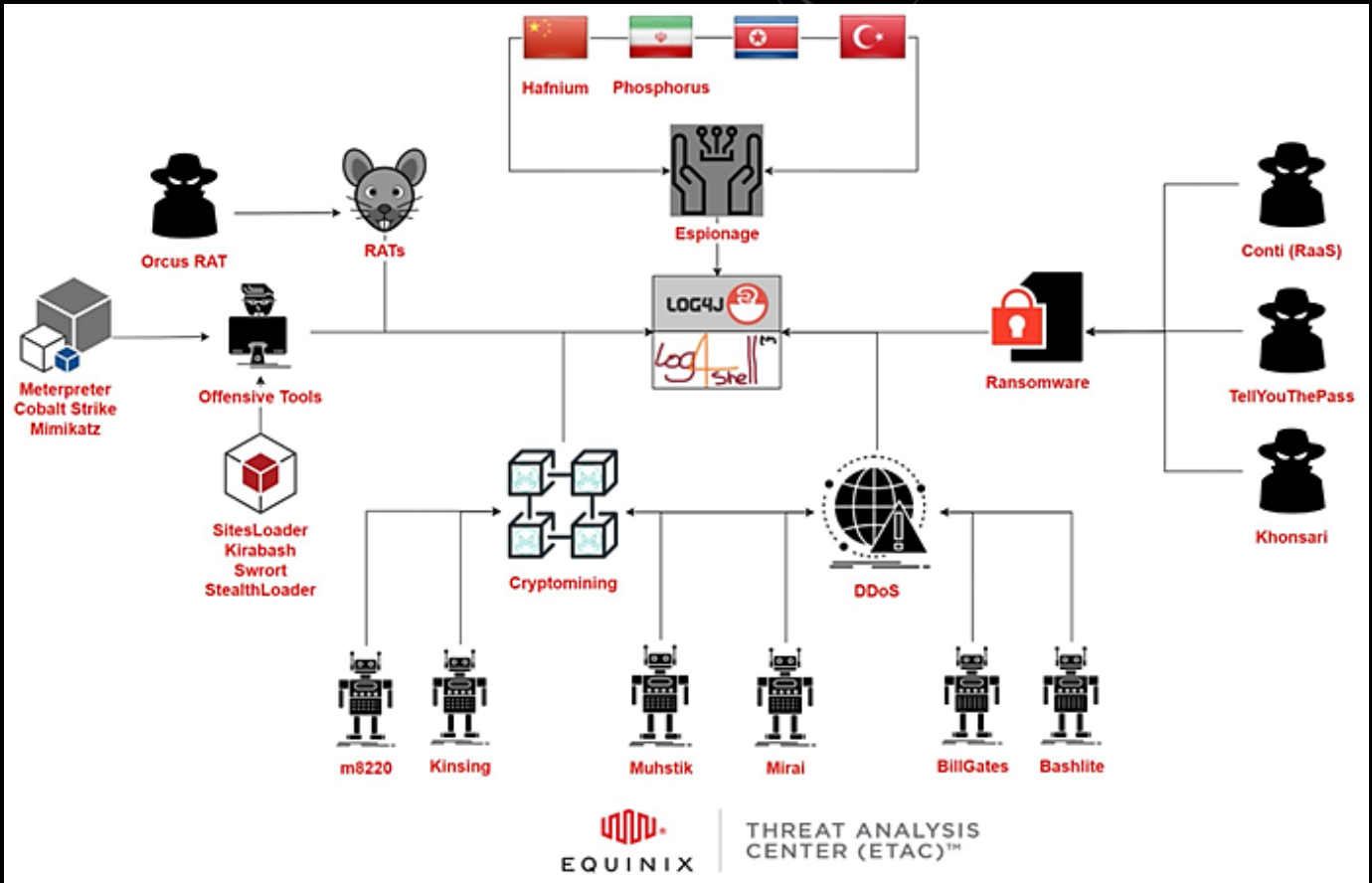
ATT&CK CAMPAIGNS

2022 Roadmap

We have several exciting adjustments to the framework on the horizon for 2022, and while we will be making some structural changes this year (Mobile sub-techniques and the introduction of Campaigns), it won't be nearly as painful as the addition of Enterprise sub-techniques in 2020. In addition to Campaigns and Mobile subs, our key adjustments this year include converting detections into objects, innovating how you can use overlays and combinations, and expanding ICS assets. We plan on maintaining the biannual release schedule of April and October, with a point release (v11.1) for Mobile sub-techniques.

HAFNIUM'S LOG4SHELL CAMPAIGN

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Command and Control
Active Scanning	Acquire Infrastructure	Exploit Public-Facing Application	Command and Scripting Interpreter	Account Manipulation	Valid Accounts	Valid Accounts	OS Credential Dumping	Software Discovery	Application Layer Protocol
Vulnerability Scanning	Virtual Private Server		PowerShell	Server Software Component			LSASS Memory		DNS
Gather Victim Org Information	Web Services			Web Shell					
				Valid Accounts					




```
                    %%%%%#########%%%%%
                 ###%%%%%##                  &%%%
            (#####%%          /.. .,,,,&      .%%
        ///(###            . ...**//((... ,     %%
     ***///(               (..***//((...*#,,,     %%
 *******                  #(#./((((#......,%#(     %
  *****                   @%##....#%%%%,,%#((     %
    ****//                %%%%,,%%%%%%**/((     #
       *////(#*             %%,%%%%%##((((     %
          ((####%              ,//////
             #####%%#,                                        **
                 ##%%%#####                              //**
                     %%%%%%%%%%%%.          ######(((
                            %%%%%%%%%%%%%%%%%%%%%

                    by Curated Intelligence
```

Log4Shell-IOCs

Members of the Curated Intelligence Trust Group have compiled a list of IOC feeds and threat reports focused on the recent Log4Shell exploit targeting CVE-2021-44228 in Log4j. (Blog | Twitter | LinkedIn)

Analyst Comments:

- 2021-12-13
  - IOCs shared by these feeds are `LOW-TO-MEDIUM CONFIDENCE` we strongly recommend `NOT` adding them to a blocklist
  - These could potentially be used for `THREAT HUNTING` and could be added to a `WATCHLIST`
  - Curated Intel members at various organisations recommend to `FOCUS ON POST-EXPLOITATION ACTIVITY` by threats leveraging Log4Shell (ex. threat actors, botnets)
  - IOCs include JNDI requests (LDAP, but also DNS and RMI), cryptominers, DDoS bots, as well as Meterpreter or Cobalt Strike
  - Critical IOCs to monitor also include attacks using DNS-based exfiltration of environment variables (e.g. keys or tokens), a Curated Intel member shared an example

[Mitigating Log4Shell and Other Log4j-Related Vulnerabilities | CISA]

Additional resources to detect possible exploitation or compromise are identified below. **Note:** due to the urgency to share this information, CISA, the FBI, NSA, ACSC, CCCS, CERT NZ, NZ NCSC, and NCSC-UK have not yet validated this content.

- Cisco Talos blog: Threat Advisory: Critical Apache Log4j vulnerability being exploited in the wild
- Curated Intelligence GitHub page: Log4Shell-IOCs (**Note:** Curated Intelligence notes that the "IOCs shared by these feeds are low-to-medium confidence we [Curated Intelligence] strongly recommend not adding them to a blocklist.")
- EmergingThreat.net: signatures to assist with detection of CVE-2021-44228 activity
- Florian Roth's GitHub pages:
  - Log4j RCE Exploitation Detection
  - signature-base/yara/expl_log4j_cve_2021_44228.yar
  - log4shell-detector

ABUSED LEGITIMATE SERVICES

Abused Legitimate Services

Legitimate third-party Platform-as-a-Service (PaaS) providers are becoming increasingly leveraged by threat actors for phishing and malware deployment. PaaS providers such as cloud instances, marketing platforms, content delivery networks (CDN), and dynamic DNS servers have been weaponised for a range of malicious activities. One of the key benefits is that they can be used to evade detection systems. This is due to the decreased likelihood of these being pre-emptively blocked because of established levels of trust and legitimate usage.

Detailed analysis in the blog here: https://blog.bushidotoken.net/2021/11/leveraging-legitimate-services-for.html

Abused Legitimate Services by Malware campaigns

Abused Legitimate Services by Phishing campaigns

ANDROID BANKING TROJANS

Common Name	AKA	Code Similarities	Associated TAs	Last Reported
Medusa	Gorgona, TangleBot	-	-	Feb-22
MoqHao	Shaoye, Xloader, Wroba.g	-	RoamingMantis	Feb-22
Hydra	-	-	-	Feb-22
FluBot	Cabassous, FakeChat	-	-	Feb-22
Vultur	-	-	-	Jan-22
Alien	-	Cerberus	-ring0-	Jan-22
BRATA	-	-	-	Jan-22

OPEN-SOURCE MALWARE

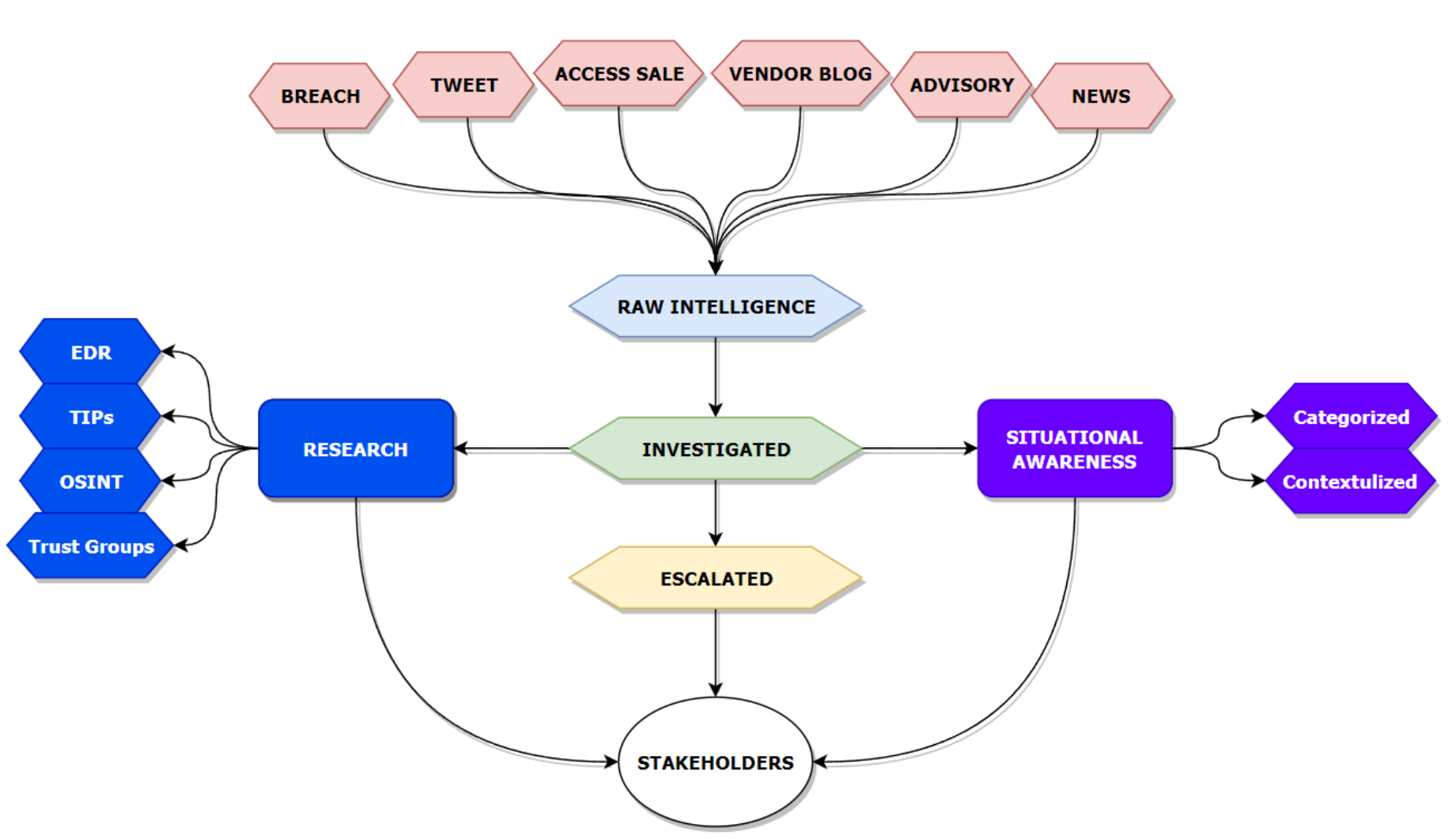
Name	Type	Platform	URL
emp3r0r	C&C framework	Linux	https://github.com/jm33-m0/emp3r0r
Shad0w	C&C framework	Windows	https://github.com/bats3c/shad0w
Empire	C&C framework	Windows	https://github.com/EmpireProject/Empire
Covenant	C&C framework	Windows	https://github.com/cobbr/Covenant
Octopus	C&C framework	Windows	https://github.com/mhaskar/Octopus
Mythic	C&C framework	Windows	https://github.com/its-a-feature/Mythic
Silent Trinity	C&C framework	Windows	https://github.com/byt3bl33d3r/SILENTTRINITY
Koadic	C&C framework	Windows	https://github.com/zerosum0x0/koadic
GRAT2	C&C framework	Windows	https://github.com/r3nhat/GRAT2
Merlin	C&C framework	Cross-platform	https://github.com/Ne0nd0g/merlin
Metasploit	C&C framework	Cross-platform	https://github.com/rapid7/metasploit-framework

FAMOUS MALWARE

Category	Name	Type	SHA256
Infamous	WannaCry	Ransomware Worm	24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C
Infamous	NotPetya	Ransomware Worm	027CC450EF5F8C5F653329641EC1FED91F694E0D229928963B30F6B0D7D3A745
Infamous	Shamoon	MBR Wiper	F1710C802CE590BC737EDA6D1845F390A7E7D2CF43313C3362768C5F9F94A807
Infamous	Destover	MBR Wiper	4D4B17DDBCF4CE397F76CF0A2E230C9D513B23065F746A5EE2DE74F447BE39B9
Infamous	EternalBlue	Exploit	85B936960FBE5100C170B777E1647CE9F0F01E3AB9742DFC23F37CB0825B30B5
Infamous	SUNBURST	Backdoor	0F5D7E6DFDD62C83EB096BA193B5AE394001BAC036745495674156EAD6557589
ICS	Stuxnet	ICS	4C3D7B38339D7B8ADF73EAF85F0EB9FAB4420585C6AB6950EBD360428AF11712
ICS	Triton	ICS	70EFBD074326E7BBD4E851DED5C362FE5FE06282ED4BBB4B9F761F1B12EE32F7
ICS	CrashOverride	ICS	12BA9887D3007B0A0713D9F1973E1176BD33ECCB017B5A7DBA166C7C172151E9
Espionage	Double Pulsar	Backdoor	27CB61D6645EB64201CB7384DD029291AC1E2110B8A5304C4D8B810F0725AEF3
Espionage	Regin	Backdoor	F1D903251DB466D35533C28E3C032B7212AA43C8D64DDF8C5521B43031E69E1E
Espionage	PlugX	RAT	B8A13C2A4E09E04487309EF10E4A8825D08E2CD4112846B3EBDA17E013C97339
Espionage	Zebrocy	Backdoor	0BE114FE30EF5042890C17033B63D7C9E0363972FCC15A61433C598DD33F49D1

ACTIONABLE INTELLIGENCE

- PIRs
- OKRs
- RFIs



THANK YOU!

twitter.com/BushidoToken

linkedin.com/in/william-t

blog.bushidotoken.net

github.com/BushidoUK