

RANSOMWARE INVESTIGATION (OSINT AND HUNTING) – OVERVIEW PT1

Joas Antonio

[https://www.linkedin.com/in/
joas-antonio-dos-santos](https://www.linkedin.com/in/joas-antonio-dos-santos)

What is Ransomware?

- Ransomware is malware that employs encryption to hold a victim's information at ransom. A user or organization's critical data is encrypted so that they cannot access files, databases, or applications. A ransom is then demanded to provide access. Ransomware is often designed to spread across a network and target database and file servers, and can thus quickly paralyze an entire organization. It is a growing threat, generating billions of dollars in payments to cybercriminals and inflicting significant damage and expenses for businesses and governmental organizations.

Types of Ransomware

Common Types of Ransomware Attacks



- 1 Crypto ransomware
- 2 Locker ransomware
- 3 Scareware
- 4 Ransomware as a Service (RaaS)
- 5 Doxware/Leakware

Types of Ransomware

1. Crypto ransomware

- The goal of crypto ransomware is to hack and encrypt the sensitive files located on the victim's computer, such as documents, pictures, or videos. While cybercriminals withhold access to these files, they don't go as far as interfering with basic computer functions like other types of ransomware. Hackers want to create a sense of panic within the user by allowing them to see their files without the ability to open their information.

2. Locker ransomware

- Locker ransomware is unique in that it solely aims to lock victims out of their computers. Hackers do this by disabling all basic computer functions with an exception for minor mouse and keyboard capabilities. Leaving the mouse and keyboard somewhat operable lets the user fulfill the demands of the cybercriminal to gain access back into their device.
- A common trend with locker ransomware is that it generally doesn't target specific files. So, the likelihood of data destruction is lower compared to other types of ransomware attacks. However, there are no guarantees when dealing with cybercriminal masterminds.

Types of Ransomware

3. Scareware

- Scareware is a malicious software created to make false claims about viruses infecting a user's computer or device. A payment is typically requested from the owner to solve the falsified issues. While some types of scareware can lock a user out of their device, others will only go as far as flooding the screen with countless pop-ups to overwhelm the user.

4. Ransomware as a Service (RaaS)

- Ransomware as a Service (RaaS) is a dark web business model created to help ransomware hackers streamline their attacks. Developers created this software to automatically carry out all aspects of a ransomware attack for the cyberthief, from sending out the ransomware to collecting payments and restoring user access.

5. Doxware or leakware

- Doxware, also known as leakware, threatens the distribution of sensitive data online, targeting people and businesses alike. Since hackers know people, and especially businesses, will do almost anything to prevent confidential and personal data from falling into the wrong hands, they often demand compensation to prevent its release.

Ransomware Report

Ransomware in 2022

<https://www.blackfog.com/the-state-of-ransomware-in-2022/>

<https://therecord.media/ransomware-tracker-the-latest-figures/>

<https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-conti-and-blackcat-lead-pack-amid-rise-in-active-raas-and-extortion-groups-ransomware-in-q1-2022>

Commons Ransomware

- [Cerber](#)
- [Bad Rabbit](#)
- [CryptoWall](#)
- [Crysis](#)
- [LockerGoga](#)
- [LeChiffre](#)
- [Petya](#)
- [NotPetya](#)
- [KeRanger](#)
- [Jigsaw](#)
- [GoldenEye](#)
- [CTB-Locker](#)
- [Maze](#)
- [Locky](#)
- [WannaCry](#)
- [ZCryptor](#)
- [TorrentLocker](#)
- [TeslaCrypt](#)
- [Spider](#)
- [Ryuk](#)

+

•

○

INVESTIGATION RANSOMWARE

APT Groups

- Groups are sets of related intrusion activity that are tracked by a common name in the security community. Analysts track clusters of activities using various analytic methodologies and terms such as threat groups, activity groups, threat actors, intrusion sets, and campaigns. Some groups have multiple names associated with similar activities due to various organizations tracking similar activities by different names. Organizations' group definitions may partially overlap with groups designated by other organizations and may disagree on specific activity.

APT Groups – List and Report

- <https://attack.mitre.org/groups/>
- <https://www.mandiant.com/resources/insights/apt-groups>
- <https://cybersophia.net/cyber-threat-intel/advanced-persistent-threat-apt-groups/>
- <https://adversary.crowdstrike.com/en-US/?L=32>
- <https://www.crowdstrike.com/resources/reports/global-threat-report/>

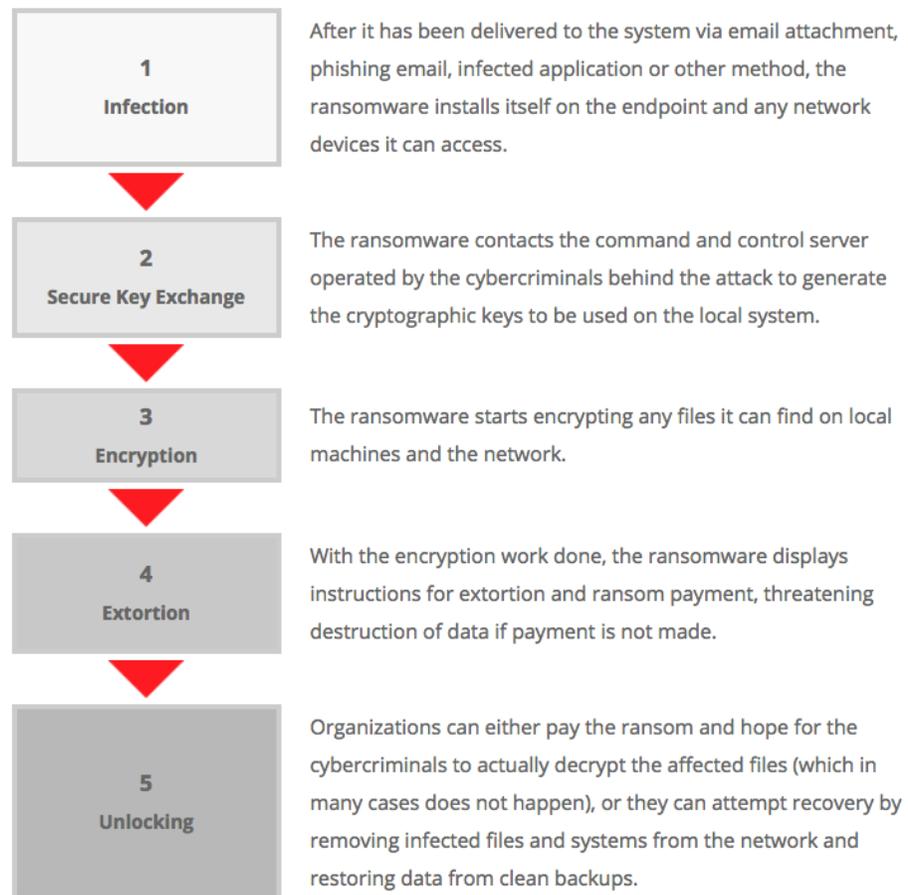
RANSOMWARE INCIDENT RESPONSE

Steps in a ransomware incident response plan

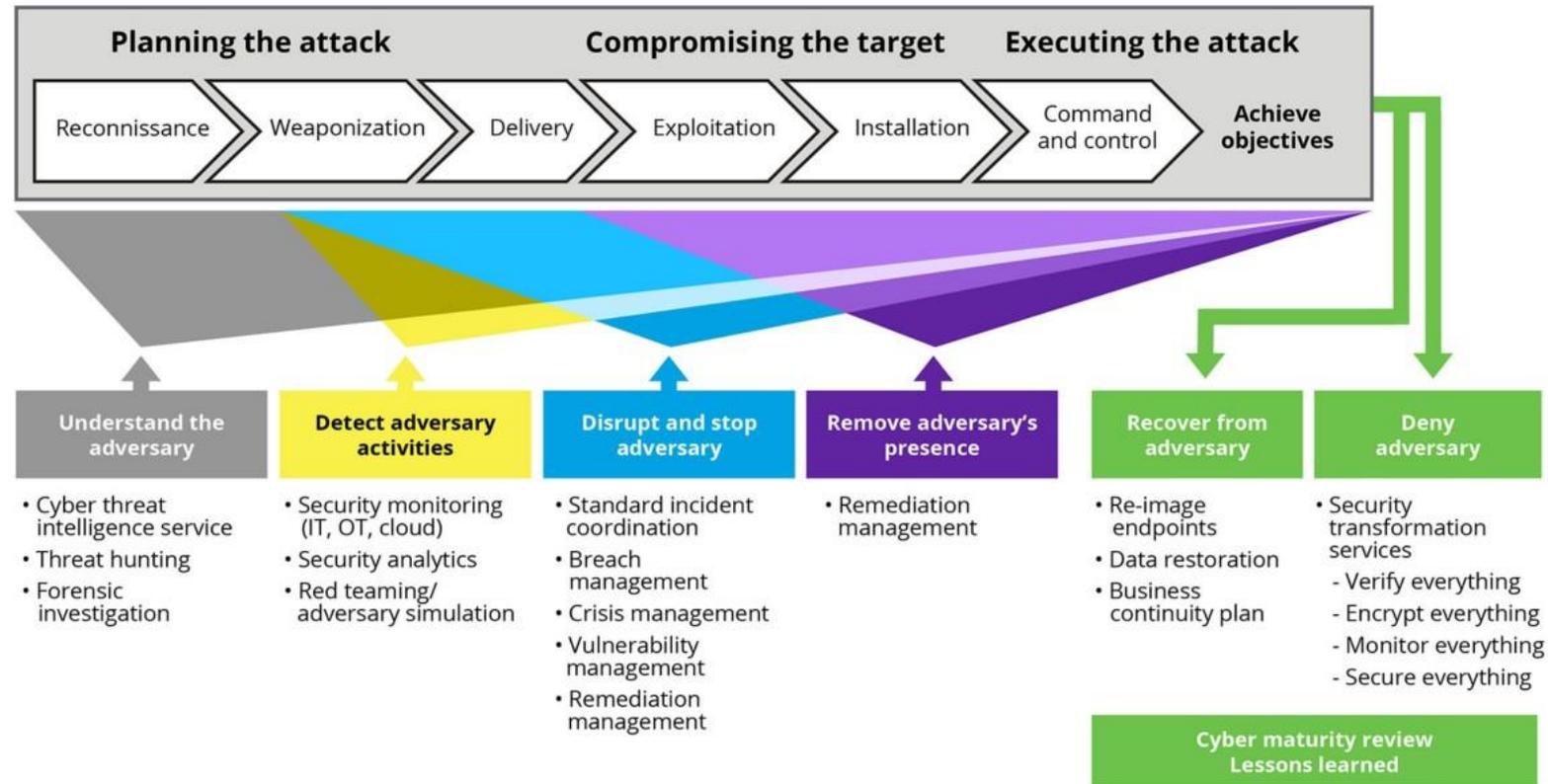


1. Validate the attack
2. Gather the incident response team
3. Quickly analyze the incident
4. Contain the incident
5. Perform a thorough investigation
6. Eradicate malware
7. Contact law enforcement
8. Perform post-incident activities
9. Perform post-mortem analysis and learn from the attack

Ransomware Process



Ransomware Attack and Recovery



OSINT – What is?

- By gathering publicly available sources of information about a particular target an attacker – or friendly penetration tester – can profile a potential victim to better understand its characteristics and to narrow down the search area for possible vulnerabilities. Without actively engaging the target, the attacker can use the intelligence produced to build a threat model and develop a plan of attack. Targeted cyber attacks, like military attacks, begin with reconnaissance, and the first stage of digital reconnaissance is passively acquiring intelligence without alerting the target.
- Gathering OSINT on yourself or your business is also a great way to understand what information you are gifting potential attackers. Once you are aware of what kind of intel can be gathered about you from public sources, you can use this to help you or your security team develop better defensive strategies. What vulnerabilities does your public information expose? What can an attacker learn that they might leverage in a social engineering or phishing attack?

OSINT Framework – What is?

- Gathering information from a vast range of sources is a time consuming job, but there are many tools to make intelligence gathering simpler. While you may have heard of tools like Shodan and port scanners like Nmap and Zenmap, the full range of tools is vast. Fortunately, security researchers themselves have begun to document the tools available.
- A great place to start is the OSINT Framework put together by Justin Nordine. The framework provides links to a large collection of resources for a huge variety of tasks from harvesting email addresses to searching social media or the dark web.

Malware Database

- <https://github.com/Endermanch/MalwareDatabase>
- <https://github.com/Pyran1/MalwareDatabase>
- <https://github.com/acastillorobles77/MalwareDatabase>
- <https://github.com/sophos/SOREL-20M>
- <https://virusshare.com/>
- <https://labs.inquest.net/>
- <https://bazaar.abuse.ch/>
- <https://www.hybrid-analysis.com/>
- <https://urlhaus.abuse.ch/>
- <https://beta.virusbay.io/>
- <https://www.virustotal.com/>

Malware Samples

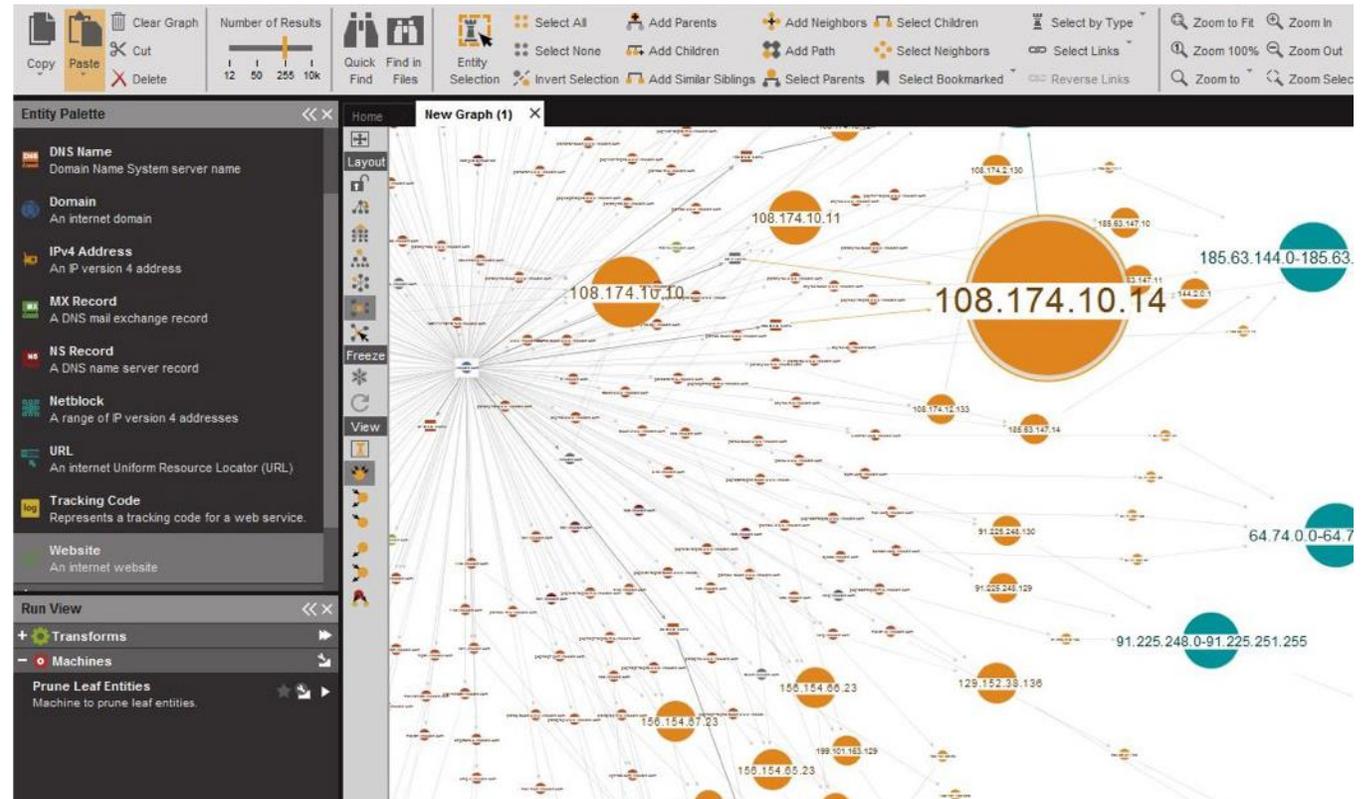
- <https://github.com/jstrosch/malware-samples>
- <https://github.com/fabrimagic72/malware-samples>
- <https://github.com/ytisf/theZoo>
- <https://github.com/mstfknn/malware-sample-library>

Create Lab

- Install Windows 7 and 10
- Install Linux or preference Kali Linux
- <https://www.sentinelone.com/labs/building-a-custom-malware-analysis-lab-environment/>
- https://www.youtube.com/watch?v=GE_aSVq8ZnQ
- https://www.youtube.com/watch?v=fLJifLf_fRE
- <https://www.youtube.com/watch?v=bBvOiADXjEQ>

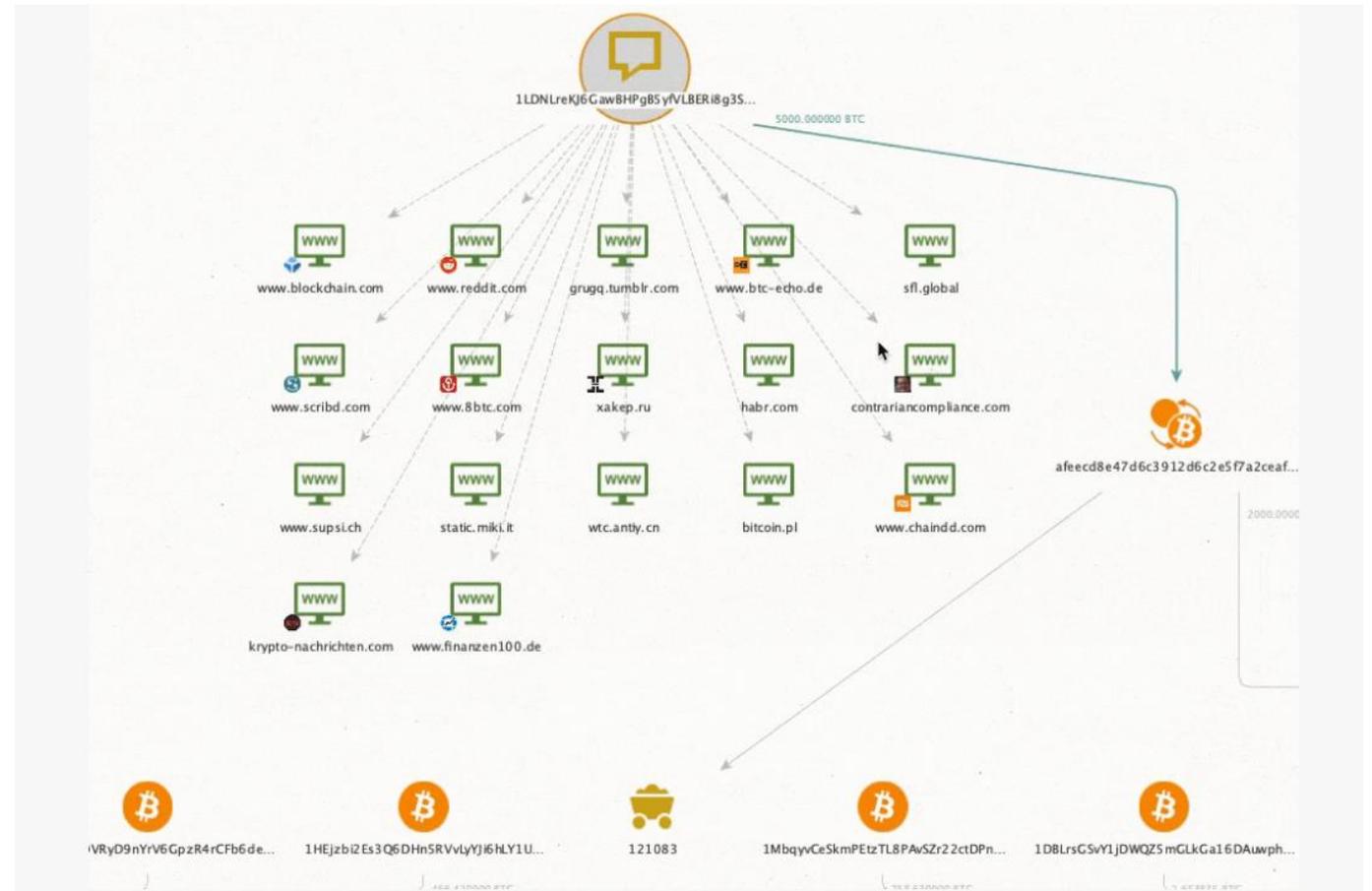
OSINT – Maltegoce Transforms

- Intezer Analyze Transforms for Maltego;
- Abuse.ch URLhaus;
- AbuseIPDB;
- ATII Hades Darkweb;
- Virus Total Premium;
- Cybersixgill;
- Att&ck MISP;
- Threat Crowd;
- Shodan;
- Crowdstrike Intel;
- Recorded Future;
- Hyas insight;
- Flashpoint;
- Hybrid Analysis;
- Threat Miner;
- Blockchain.info
- Cipher Trace;
- Tatum Blockchain;



OSINT – Maltegoce Cryptocurrency 1

Blockchain.com (formerly Blockchain.info) is a provider of cryptocurrency blockchain explorer services. It's a platform that offers ways to buy, hold, and use cryptocurrency. It creates a financial system for the internet that empowers anyone in the world to control their money. Over 50+ million customers have signed up to use the Blockchain.com platform. It's a fast and easy way to buy bitcoin, trade crypto, send, receive, secure, and borrow digital currencies.

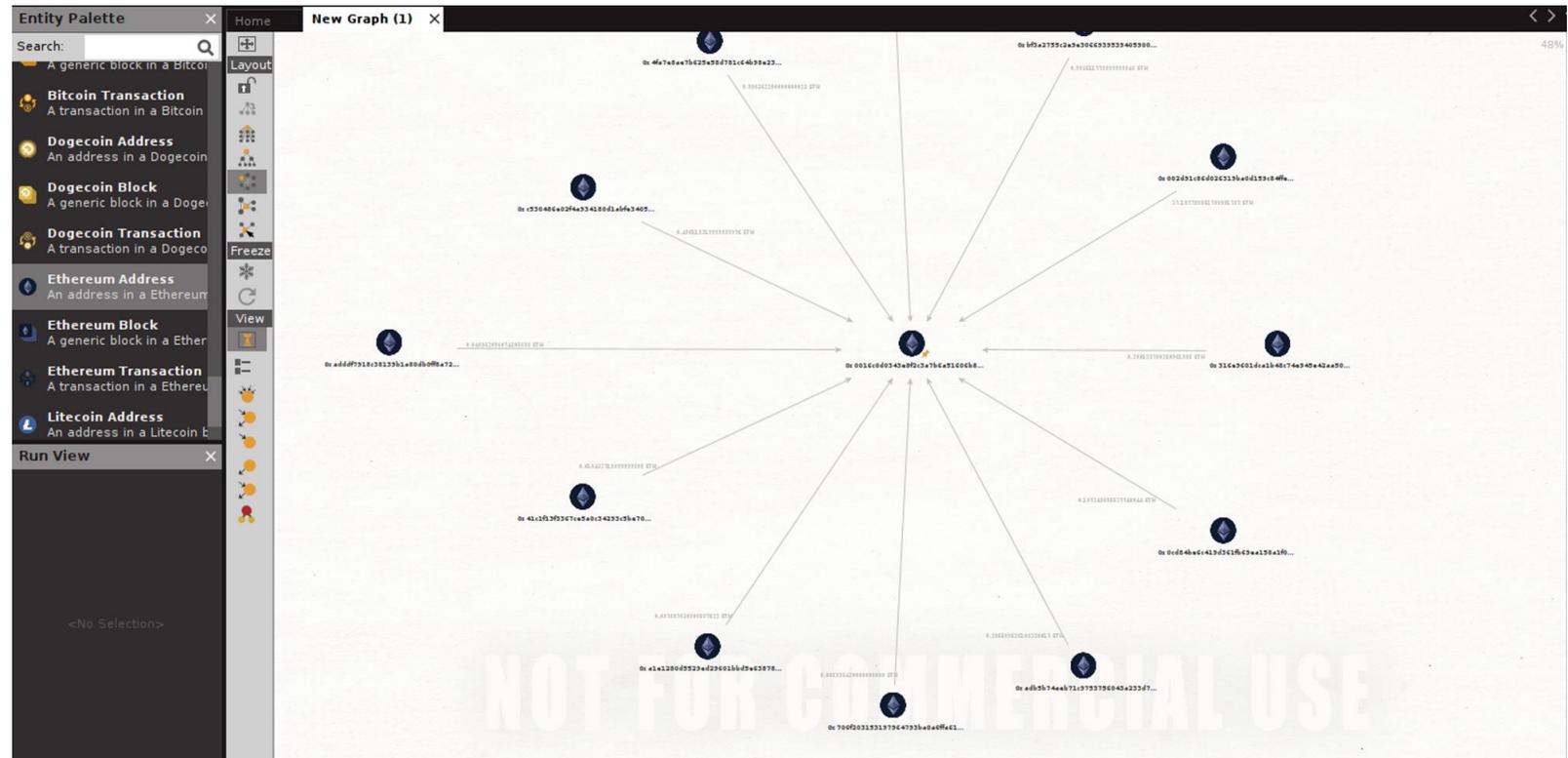


OSINT – Maltegoce Cryptocurrency 2

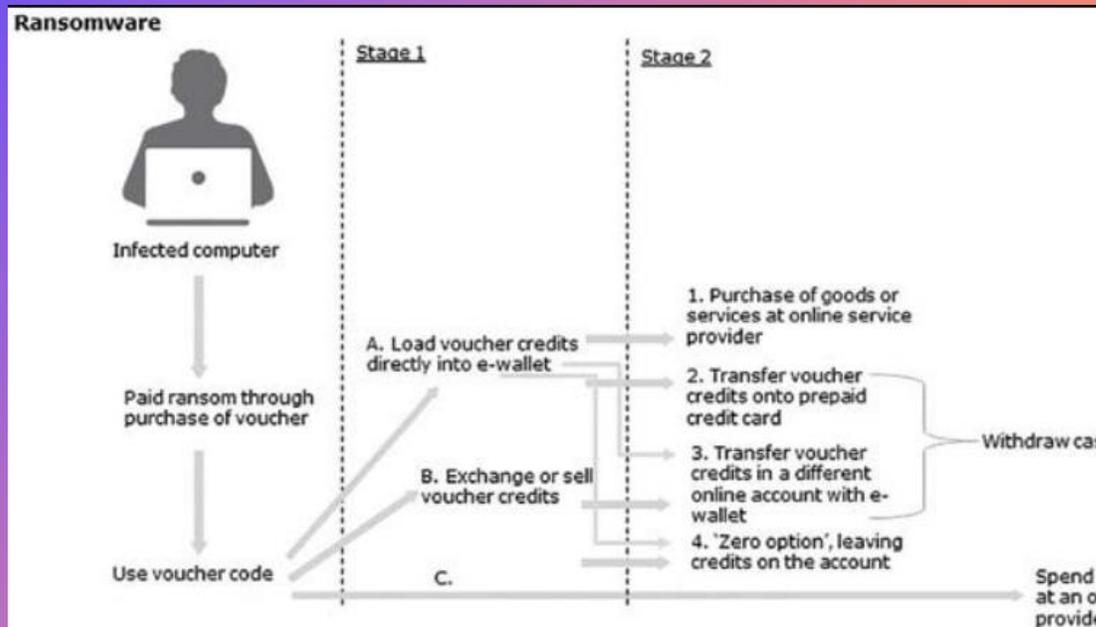
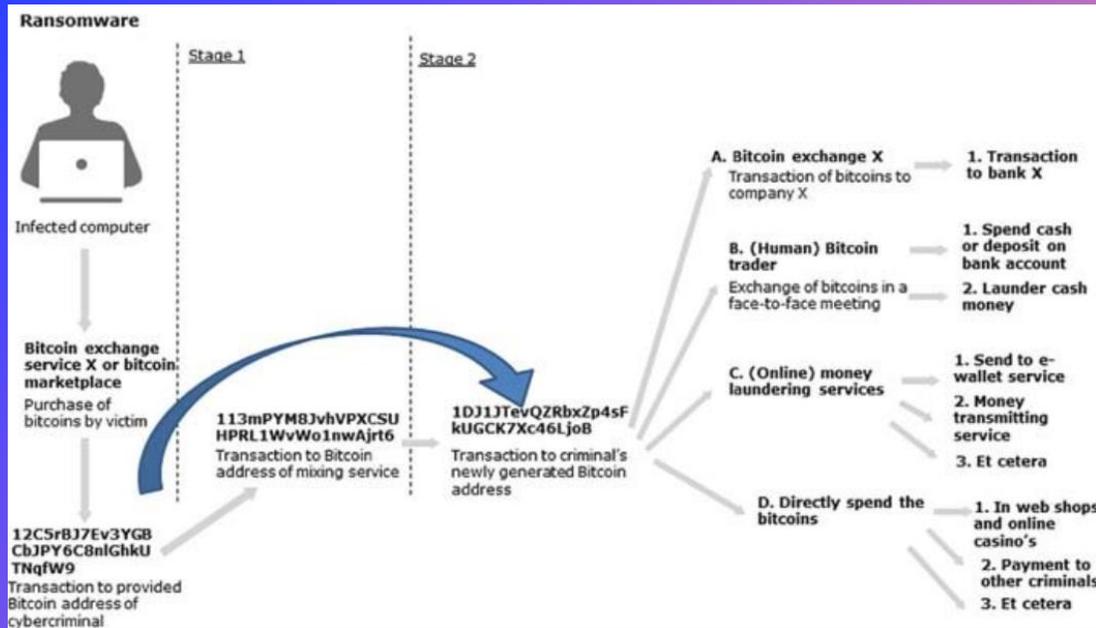
<https://sociallinks.io/webinars/analysing-cryptocurrencies-and-investigating-blockchains>

<https://www.youtube.com/watch?v=A7XhEvAgYz4>

<https://alphasec.io/how-to-visualize-ethereum-transactions-using-maltego/>



Model for the Money laundering of Ransomware



- **Anonymity:** Bitcoin provides anonymity when payments are received and when they are cashed out. That's because bitcoin accounts and money transfers are difficult to trace and depend largely on the cybercriminal being sloppy with operations security.
- **Global Currency:** Hackers typically prey on out-of-country targets and need a fast, untraceable method to transfer funds across nations without worrying about account freezes. Bitcoin is used as a global currency because you don't need to worry about the exchange rates between your home country's currency and US dollars.
- **Ease of Payments:** In the past, hackers used to rely on gift cards for payment. This was troublesome on many levels — for instance, gift cards can't be used globally, and criminals needed to come up with mailing addresses that can't be traced. Bitcoin and the higher profile of cryptocurrency have contributed to the rise in ransomware, as well as hackers' ability to use extortion to elicit payments. One example occurred after the Ashley Madison website breach, when hackers threatened some users with a bitcoin ransom or have their identities revealed as adulterers. Another tactic involved using malicious emails to threaten a distributed denial-of-service attack on an organization's network unless a bitcoin payment was made.

Analyzing Wallet Addresses using Blockchain Explorers

- In cryptocurrency investigations, blockchain ledgers play a significant role. To render it simpler to comprehend and make sense of the information, investigators use Wallet explorers to conduct analysis on wallet addresses and transactions.
- Transaction analysis is crucial in cryptocurrency investigations since it not merely permits investigators to follow the money, but also determine the source and what sort of tools the suspect employed
- One of the more known Explorers is Blockchain.com. It allows us to look up the wallet address and see all of its past transactions. It also shows how much currency it currently holds. Blockchain transactions are simple to track in the case of public ledgers like Bitcoin or Ethereum.
- WalletExplorer
- BitcoinWho'sWho
- BitcoinAbuse
- IntelX

Wallet explorers usually update in real-time with the details of each transaction, comprising of:

- Hash: The transaction ID which serves as a way to look up a particular transaction on the blockchain. (Not to be confused with Cryptographic Hashes)
- From/To: The sender's address and the recipient's address.
- Time Stamp: Each block includes the precise time for when the transaction entered the blockchain. Thus, the time the block was mined.
- Actual Cost/Fee: The price of the transaction.
- Transaction Receipt Status: Confirmation of the transaction's status.
- Value: How much cryptocurrency was sent and the equivalent USD value.

IoCs Ransomware

- Indicators of compromise (IoCs) are clues and evidence of a data breach in the form of digital breadcrumbs. These indicators can tell us whether a cyberattack has occurred, who was behind them and what tools may have been used. This information is generally obtained from software, including anti-malware and antivirus systems.
- Some of the most common IoCs to watch for are:
 1. Unusual traffic patterns between internal systems
 2. Unusual usage patterns for privileged accounts
 3. Administrative access to your network from unsuspected geographical locations
 4. A spike in database read volumes
 5. A high rate of authentication attempts and failures
 6. Unusual configuration changes
 7. C2 Servers Ips
 8. Ethereum or Bitcoin Wallets
 9. Hashes File

<https://www.packetlabs.net/posts/indicators-of-compromise-ioc/>

Example IoCS Ransomwar: <https://github.com/sophoslabs/IoCs/blob/master/Ransomware-Ryuk.csv>

Wallet trace transactions

	Address	Min Hop Depth (1-based)	Max Hop Depth (1-based)	Amount received	Currency symbol	Address type	Address annotation
1	1KHD1zT1EhqKjytEepkFGSfEGEBwKGs6QN	10	10	1.780452	BTC	pubkeyhash	
2	1NDyJtNTjmwk5xPNhigAMu4HDHigtobu1s	3	10	0.644469	BTC	pubkeyhash	Binance,Exchange Wallet
3	1NWJd7BfJLJrEcGiGfFqbhyaiusWwaZS1	1	4	0.544072	BTC	pubkeyhash	
4	36BruGMJkQRFjpPKVnYVpjzkaGx1wodloX	5	10	0.404585	BTC	scripthash	
5	3EAXp9ZL7TH8qDtG8KEysefDw5yA9dYhjE	9	10	0.396799	BTC	scripthash	
6	1DHs9JWt3YJGoHDqxqpbWwjuxD4EgoAFyY	9	10	0.291171	BTC	pubkeyhash	
7	3Joez1Ws1mBU1DTM5z4JwjWe2HyNn8ZVkJ	6	10	0.266479	BTC	scripthash	
8	3FePGNNaZcY51i9gtGFsKy9c9R2yTQAE2e	6	10	0.219587	BTC	scripthash	
9	37JnxyGBpy4dq32siHaD4oPpZsdVuY2eRC	8	10	0.155851	BTC	scripthash	
10	3EH5knUe7oy8tjHUpBGwekL6cBmi4UNxpG	10	10	0.151085	BTC	scripthash	

Visual tools are beneficial when investigating addresses and transactions. Using Coinpath[®] technology, anyone can build visual tools to understand the money flow. We have built one on our Bitquery explorer. You can visualize all the incoming and outgoing transactions from the hacker's address here.

Today, bitcoin blockchain confirms ~10 million transactions every month. All these transactions are visible on the bitcoin blockchain. However, the blockchain only store addresses, public keys, and not real-world identities. Therefore, Virtual asset service providers (VASP) are the primary way to link real-world identities with bitcoin transactions. For example, VASPs such as Exchanges, wallets, custodians provide cryptocurrency services to retail users and businesses. Most of these services implement KYC (Know-your-customer) solutions. Therefore, linking real-world identity with bitcoin addresses and transactions.

SIEM Splunk Investigation

The screenshot shows the Splunk Malware Analysis interface. The search bar contains the following query: `sourcetype="xmlwineventlog:microsoft-windows-sysmon/operational" [search sourcetype="xmlwineventlog:microsoft-windows-sysmon/operational" EventDescription="File Create Time" | streamstats time_window=1m count(EventDescription) AS "new_files" | search new_files>10 | fields + Image] | stats last(Image) as File by sha1, _time, ParentCommandLine`. The search results show 86 events from August 21, 2016, to August 24, 2016. The results table displays columns for sha1, _time, ParentCommandLine, and File.

sha1	_time	ParentCommandLine	File
8939CF35447B22DD2C6E6F443446ACC1BF986D58	2016-08-22 17:07:28	"C:\Windows\System32\rundll32.exe" C:\Users\GORT~1.BER\AppData\Local\Temp\RNNKSV~1.DLL,qwerty 323	C:\Windows\SysWOW64\rundll32.exe
F9E5ADC6036B989A5759D551C181352282A68E55	2016-08-22 00:37:47	"C:\Windows\System32\WScript.exe" "C:\Users\gort.BERT\AppData\Local\Temp\Temp1_Label148.zip\569195505910.wsf"	C:\Users\gort.BERT\AppData\Local\Temp\QlqJuiP.exe
F9E5ADC6036B989A5759D551C181352282A68E55	2016-08-22 00:40:05	"C:\Windows\System32\WScript.exe" "C:\Users\gort.BERT\AppData\Local\Temp\Temp1_Label148.zip\569195505910.wsf"	C:\Users\gort.BERT\AppData\Local\Temp\QlqJuiP.exe
F9E5ADC6036B989A5759D551C181352282A68E55	2016-08-22 00:41:44	"C:\Windows\System32\WScript.exe" "C:\Users\gort.BERT\AppData\Local\Temp\Temp1_Label148.zip\569195505910.wsf"	C:\Users\gort.BERT\AppData\Local\Temp\QlqJuiP.exe

https://www.splunk.com/en_us/blog/industries/detecting-ransomware-attacks-with-splunk.html

Capturing Windows Memory Using Winpmem

- Winpmem is a part of the Pmem Suite, a suite of memory acquisition tools for Windows, Linux, and Mac OS. You can download the latest release of winpmem from here: <https://github.com/Velocidex/c-aff4/releases>.
- Run Winpmem
- First, after I staged my malicious activity, I downloaded winpmem 3.3 RC3 onto the victim Windows machine. From there, I opened a command-line terminal and executed the program:
- `C:\winpmem_v3.3.rc3.exe --output memdump.raw --format raw --volume_`
- The `--output mem.raw` option was used to name the output as `memdump.raw`. The `--format raw` and `--volume_format raw` options were used to output the memory in raw format (as opposed to something like aff4). After several minutes, the memory dump finished. I then transferred the raw memory file, `memdump.raw`, to my Kali machine.
- <https://blog.cyberhacktics.com/memory-forensics-on-windows-10-with-volatility/>
- <https://github.com/Velocidex/c-aff4/releases>

Volatility Ransomware

- Identifying Malicious Processes (`python3 vol.py -f <filename> pslist`)
- Below are the keys headers from 'pslist' that you will need to understand when you begin using the tool:
 - PID - Process ID number
 - PPID - Parent process ID number
 - ImageFileName - Name of the running process
 - Offset - Hexadecimal value representing the location in memory the process is running
 - CreateTime - Time process started
 - ExitTime - Time process ended

<https://book.hacktricks.xyz/generic-methodologies-and-resources/basic-forensic-methodology/memory-dump-analysis/volatility-examples#installation>

<https://github.com/volatilityfoundation/volatility/wiki/>

Volatility Ransomware 2



PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime
4	0	System	0xbe0a574ac040	153	-	N/A	False	2021-05-20 07:28:25.000000	N/A
* 312	4	smss.exe	0xbe0a58d18800	2	-	N/A	False	2021-05-20 07:28:25.000000	N/A
** 492	312	smss.exe	0xbe0a598cd080	0	-	1	False	2021-05-20 07:28:39.000000	2021-05-20 07:28:40.000000
*** 584	492	winlogon.exe	0xbe0a5994e800	6	-	1	False	2021-05-20 07:28:40.000000	N/A
**** 664	584	userinit.exe	0xbe0a5a5d6800	0	-	1	False	2021-05-20 07:31:33.000000	2021-05-20 07:31:49.000000
***** 1900	664	explorer.exe	0xbe0a5a5ed800	112	-	1	False	2021-05-20 07:31:33.000000	N/A
***** 5384	1900	MSASCuil.exe	0xbe0a5ae3a800	5	-	1	False	2021-05-20 07:32:06.000000	N/A
***** 5408	1900	chrome.exe	0xbe0a5c67c080	26	-	1	False	2021-05-26 12:27:16.000000	N/A
***** 6112	5408	chrome.exe	0xbe0a604ae200	10	-	1	False	2021-05-26 12:27:17.000000	N/A
***** 1028	5408	chrome.exe	0xbe0a585fc800	6	-	1	False	2021-05-26 12:27:17.000000	N/A
***** 1832	5408	chrome.exe	0xbe0a5cba3080	12	-	1	False	2021-07-06 17:14:35.000000	N/A
***** 4112	5408	chrome.exe	0xbe0a59b65080	13	-	1	False	2021-05-26 12:27:23.000000	N/A
***** 8116	5408	chrome.exe	0xbe0a57eb4800	8	-	1	False	2021-05-26 12:27:16.000000	N/A
***** 4856	5408	chrome.exe	0xbe0a5cf63080	6	-	1	False	2021-05-26 12:27:19.000000	N/A
***** 6780	5408	chrome.exe	0xbe0a5fb90300	22	-	1	False	2021-05-26 12:27:17.000000	N/A
***** 5428	1900	vmtoolsd.exe	0xbe0a5ae07800	9	-	1	False	2021-05-20 07:32:06.000000	N/A
***** 6648	1900	ProcessHacker.	0xbe0a5a9f4800	18	-	1	False	2022-01-13 09:52:53.000000	N/A
**** 924	584	dwm.exe	0xbe0a59ab84c0	11	-	1	False	2021-05-20 07:28:44.000000	N/A
*** 516	492	csrss.exe	0xbe0a59900280	15	-	1	False	2021-05-20 07:28:39.000000	N/A
* 2228	4	MemCompression	0xbe0a59446040	24	-	N/A	False	2021-05-20 07:28:46.000000	N/A
428	412	csrss.exe	0xbe0a59215080	11	-	0	False	2021-05-20 07:28:36.000000	N/A
500	412	wininit.exe	0xbe0a598c2080	1	-	0	False	2021-05-20 07:28:39.000000	N/A
* 652	500	lsass.exe	0xbe0a599cb080	8	-	0	False	2021-05-20 07:28:41.000000	N/A
* 636	500	services.exe	0xbe0a599a2800	9	-	0	False	2021-05-20 07:28:41.000000	N/A
** 4356	636	svchost.exe	0xbe0a60833400	6	-	0	False	2021-05-26 12:20:35.000000	N/A
** 2056	636	VGAuthService.	0xbe0a59cb1800	2	-	0	False	2021-05-20 07:28:46.000000	N/A
** 648	636	sedsv.exe	0xbe0a59150080	7	-	0	False	2021-05-20 07:30:50.000000	N/A
** 1804	636	MsMpEng.exe	0xbe0a59cb5800	13	-	0	False	2021-05-20 07:28:46.000000	N/A
** 6540	636	svchost.exe	0xbe0a61289080	7	-	0	False	2022-01-13 09:53:19.000000	N/A
** 2064	636	vm3dservice.ex	0xbe0a59caf800	2	-	0	False	2021-05-20 07:28:46.000000	N/A
*** 2384	2064	vm3dservice.ex	0xbe0a59d92800	2	-	1	False	2021-05-20 07:28:47.000000	N/A
** 3600	636	sppsvc.exe	0xbe0a5d135280	4	-	0	False	2022-01-13 09:53:29.000000	N/A
** 1684	636	spoolsv.exe	0xbe0a596bf800	14	-	0	False	2021-05-20 07:28:45.000000	N/A
** 1948	636	svchost.exe	0xbe0a59cea380	15	-	0	False	2021-05-20 07:28:46.000000	N/A
** 800	636	svchost.exe	0xbe0a59a4a800	28	-	0	False	2021-05-20 07:28:44.000000	N/A
** 2724	636	dllhost.exe	0xbe0a595f9080	12	-	0	False	2021-05-20 07:28:48.000000	N/A
** 1452	636	svchost.exe	0xbe0a58de7300	8	-	0	False	2021-05-20 07:28:44.000000	N/A
*** 6188	1452	audiodg.exe	0xbe0a5ee59080	7	-	0	False	2021-07-06 17:16:18.000000	N/A

- Using 'pstree' is a great way to spot these malicious processes masquerading as legitimate Windows processes. (`python3 vol.py -f <filename> pstree`)

Volatility Ransomware 3

- To view the network connections associated with the RAM dump that is being analyzed use the following command: **(python3 vol.py -f <filename> netscan)**
 - Offset - Location in memory
 - Proto - Network protocol used by process
 - LocalAddr - Source address of network connection
 - LocalPort - Source port of network connection
 - ForeignAddr - Destination address of network connection
 - ForeignPort - Destination address of network connection
 - State - State of network connection i.e. established, closed or listening
 - PID - Process ID of associated process
 - Owner - Account associated with process
 - Created - Time network connection has initiated

The image shows two screenshots of web-based tools. The top screenshot is from Symantec's WebPulse tool, titled 'Solicitação de análise de site do WebPulse'. It features a search bar with the URL 'http://sitereview.symantec.com/#/' and a 'Verificar categoria' button. The bottom screenshot is from IBM X-Force Exchange, titled 'Research, Collaborate and Act on threat intelligence'. It shows a search bar with the text 'Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...' and a magnifying glass icon. Below the search bar is the URL 'https://exchange.xforce.ibmcloud.com/'.

Volatility Ransomware 4



```
root@kali:~/volatility# ls -ls procdump/
file.0xdb8980599990.0xdb89804f2db0.ImageSectionObject.ntdll.dll.img
file.0xdb8980509950.0xdb8980509bd0.ImageSectionObject.ntdll.dll.img
file.0xdb898121f470.0xdb89812bad0.ImageSectionObject.rpccrt4.dll.img
file.0xdb8981220bc0.0xdb89812c1db0.ImageSectionObject.SHCORE.dll.img
file.0xdb89812553d0.0xdb8981462c70.ImageSectionObject.advapi32.dll.img
file.0xdb898126a5e0.0xdb897ff44c40.ImageSectionObject.windows.storage.dll.img
file.0xdb8981280b0.0xdb898127b010.ImageSectionObject.wow64.dll.img
file.0xdb898128ad0.0xdb898128cb0.ImageSectionObject.wow64cpu.dll.img
file.0xdb898128f1a0.0xdb8981313ac0.ImageSectionObject.ws2_32.dll.img
file.0xdb89812bcef0.0xdb89812bb140.ImageSectionObject.win32u.dll.img
file.0xdb89812c9430.0xdb89812208c0.ImageSectionObject.gdi32full.dll.img
file.0xdb89812fc700.0xdb89812a0de0.ImageSectionObject.wow64win.dll.img
file.0xdb8981303080.0xdb898121f790.ImageSectionObject.user32.dll.img
file.0xdb8981304310.0xdb8981310950.ImageSectionObject.profpapi.dll.img
file.0xdb898130680.0xdb8981304010.ImageSectionObject.crypt32.dll.img
file.0xdb898131070.0xdb898128fa0. ImageSectionObject.shlwapi.dll.img
file.0xdb8981316480.0xdb8981312010.ImageSectionObject.powrprof.dll.img
file.0xdb8981369af0.0xdb89813c0010.ImageSectionObject.winnsi.dll.img
file.0xdb89813bb90.0xdb89813a8cc0.ImageSectionObject.cryptsp.dll.img
file.0xdb89813bea60.0xdb89813254d0.ImageSectionObject.OnDemandConnRouteHelper.dll.img
file.0xdb89813bfe0.0xdb8981396ab0.ImageSectionObject.urlmon.dll.img
file.0xdb89813cb00.0xdb8981364500.ImageSectionObject.rsaenh.dll.img
file.0xdb89813d980.0xdb89813d140.ImageSectionObject.kernel32.dll.img
file.0xdb89813fd210.0xdb8981392ae0.ImageSectionObject.gdi32.dll.img
file.0xdb898142ef10.0xdb898142d010.ImageSectionObject.msvc_win.dll.img
file.0xdb89814306c0.0xdb898142f010.ImageSectionObject.combase.dll.img
file.0xdb8981432b70.0xdb8981432710.ImageSectionObject.oleaut32.dll.img
file.0xdb898143bd0.0xdb8981449a40.ImageSectionObject.urtbase.dll.img
file.0xdb898143bd0.0xdb898143ade0.ImageSectionObject.kernel.appcore.dll.img
file.0xdb898143c760.0xdb8981439de0.ImageSectionObject.shell32.dll.img
file.0xdb898143d900.0xdb898143d470.ImageSectionObject.msasn1.dll.img
file.0xdb898143fa0.0xdb898143ee20.ImageSectionObject.msvcrt.dll.img
file.0xdb89814539e0.0xdb8981262010.ImageSectionObject.nsi.dll.img
file.0xdb8981453ef0.0xdb8981453ae0.ImageSectionObject.sechost.dll.img
file.0xdb89814555f0.0xdb89814519d0.ImageSectionObject.kernelbase.dll.img
file.0xdb8981455a20.0xdb8981255010.ImageSectionObject.cfgmgr32.dll.img
file.0xdb8981466be0.0xdb89814520e0.ImageSectionObject.sspicli.dll.img
file.0xdb898148a140.0xdb8981425e20.ImageSectionObject.bcryptprimitives.dll.img
file.0xdb898157cef0.0xdb898157ca20.ImageSectionObject.cryptbase.dll.img
file.0xdb8981875d40.0xdb897fcb9e0.ImageSectionObject.IPHLPAPI.DLL.img
file.0xdb8981add20.0xdb89820bc570.ImageSectionObject.wininet.dll.img
file.0xdb898212e90.0xdb89820b3740.ImageSectionObject.wtsapi32.dll.img
file.0xdb8982488570.0xdb89827b8e20.ImageSectionObject.bcrypt.dll.img
file.0xdb89826b1dd0.0xdb89827ea950.ImageSectionObject.iertutil.dll.img
file.0xdb89827bfe0.0xdb89813b31e0.ImageSectionObject.mswsock.dll.img
file.0xdb89829eab10.0xdb89818781a0.ImageSectionObject.userenv.dll.img
file.0xdb8982c24ef0.0xdb8982847db0.ImageSectionObject.dnsapi.dll.img
file.0xdb8982c26e80.0xdb89813ba4b0.ImageSectionObject.winhttp.dll.img
file.0xdb898437e80.0xdb89805ed4f0.ImageSectionObject.smsfdr.exe.img
file.0xdb898437e80.0xdb8980aa1a20.DataSectionObject.smsfdr.exe.dat
```

- Using the commands covered in this article should put you in a good position to start identifying potential malware running in memory on a device. Using ‘netscan’ I was able to identify a process named ‘smsfwder.exe’ that was making some malicious network connections to known C2 infrastructure. As part of my investigation using Volatility, I can extract this process for further analysis using a feature called ‘procdump’.
- **python3 vol.py -f <filename> -o <Directory to dump process> dumpfiles -pid <PID>**

Volatility Ransomware 5

```
Volatility Foundation Volatility Framework 2.4
ImageBase      Name      Result
-----
----- System      Error: PEB at 0x0 is unavailable
0x0000000047c50000 smss.exe  OK: executable.256.exe
0x000000004a3e0000 csrss.exe OK: executable.348.exe
0x00000000ff9c0000 wininit.exe OK: executable.400.exe
0x000000004a3e0000 csrss.exe OK: executable.408.exe
0x00000000ffa10000 winlogon.exe OK: executable.444.exe
[snip]
```

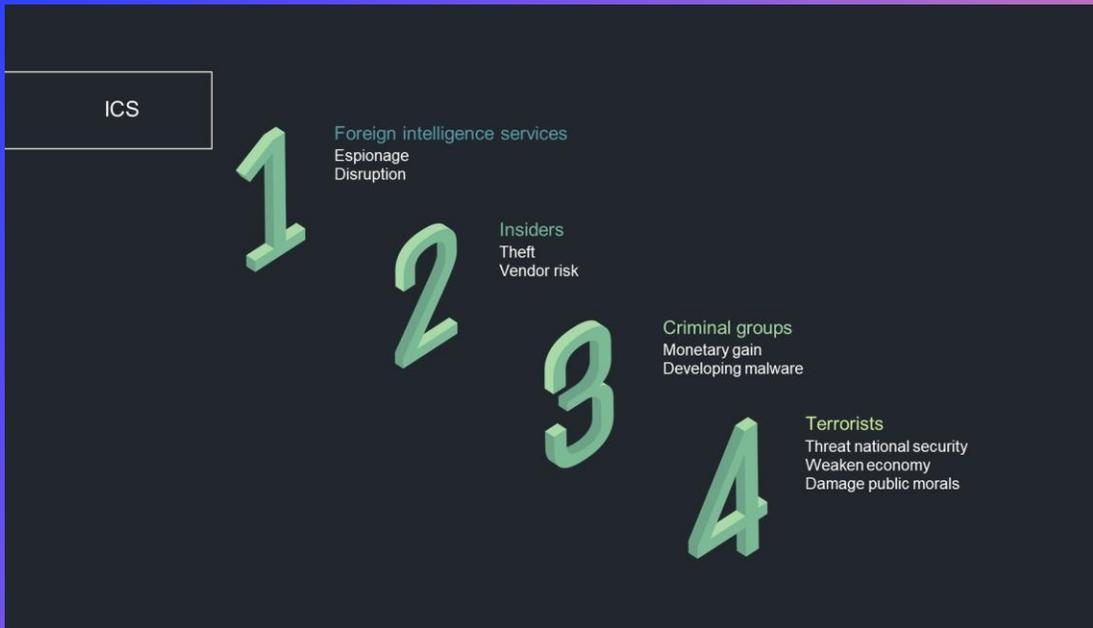
```
$ python vol.py -f memory.dmp --profile=Win7SP1x64
  procdump --offset=0x000000003e1e6b30
  --dump-dir=OUTDIR/
```

```
Volatility Foundation Volatility Framework 2.4
Process (V)      ImageBase      Name      Result
-----
0xfffffa8002be6b30 0x0000000000400000 warrant.exe OK: executable.3036.exe
```

- To dump a process's executable, use the procdump command. Optionally, pass the --unsafe or -u flags to bypass certain sanity checks used when parsing the PE header. Some malware will intentionally forge size fields in the PE header so that memory dumping tools fail.
- **python3 vol.py -f memory.dmp --profile=Win7SP1x64 procdump --dump-dir=OUTDIR/**
- Upload executable in virus total for analyze

The screenshot shows the VirusTotal interface for a file named 'winlogon.exe'. At the top, a red circle with the number '29' indicates that 29 security vendors have flagged this file as malicious. Below this, there are tabs for 'DETECTION', 'DETAILS', 'RELATIONS', 'BEHAVIOR', and 'COMMUNITY'. The 'DETECTION' tab is active, displaying a table of detections from various vendors. The table has columns for the vendor name, the detection name, and the detection ID. The vendors listed include Ad-Aware, ALYac, BitDefender, Cybereason, eScan, Fortinet, Kaspersky, K7AntiVirus, K7GW, Lionic, McAfee, and McAfee-GW-Edition. Each entry shows a red circle with a white exclamation mark, indicating a detection.

Vendor	Detection Name	Detection ID
Ad-Aware	Trojan-GenerikKD.41932477	Alibaba
ALYac	Trojan-GenerikKD.41932477	Arcabit
BitDefender	Trojan-GenerikKD.41932477	Comodo
Cybereason	Unsafe	Emisoft
eScan	Trojan-GenerikKD.41932477	FileEye
Fortinet	PossibleThreat	GData
Kaspersky	Trojan-MS32-Patched	K7AntiVirus
K7GW	Blackware (D0404F71)	Kingsoft
Lionic	Trojan-MS32-Generik.415	MAX
McAfee	Artemis32CFA83F5A8	McAfee-GW-Edition

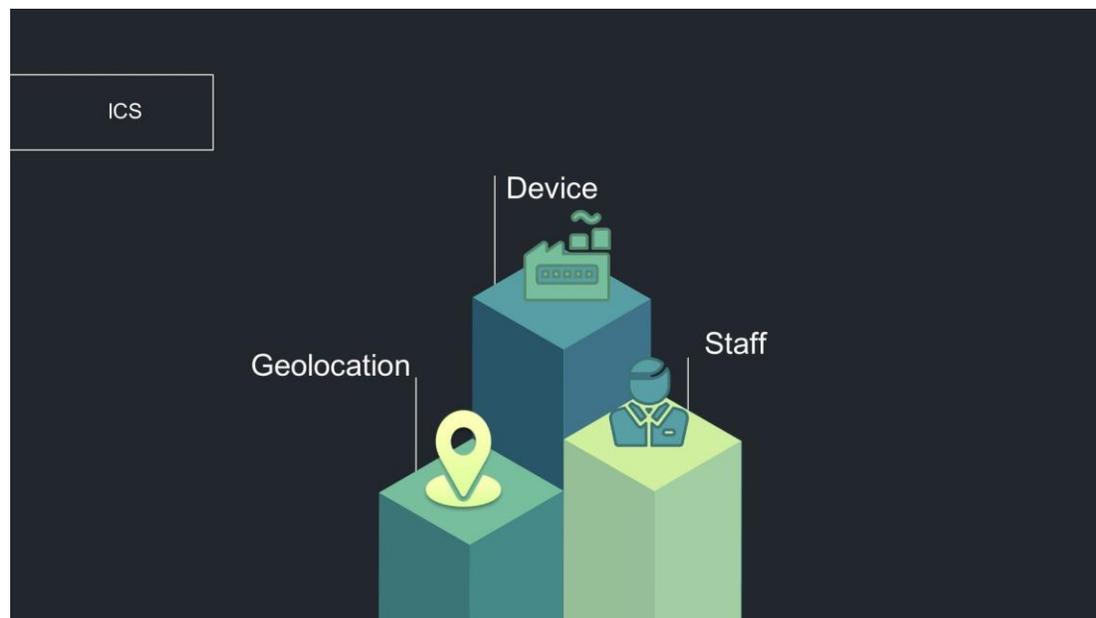


Essential Critical Infrastructure Workers

- It's perfect moment to remind about MITRE ATTACK for ICS, it describes every step of attack on SCADA/ICS devices.
- https://collaborate.mitre.org/attackics/index.php/Initial_Access
- <https://www.offensiveosint.io/offensive-osint-s01e03-intelligence-gathering-on-critical-infrastructure-in-southeast-asia/>



Geolocation IP



- A Geolocation OSINT Tool. Offers geolocation information gathering through social networking platforms.
- <https://www.geocreepy.com/>
- MaxMind is one of the leading providers of IP intelligence and online fraud detection tools. MaxMind provides IP intelligence through their GeoIP brand. Over 5,000 companies use GeoIP data to locate their internet visitors and show them relevant content and ads, enforce digital rights, and efficiently route internet traffic. Businesses can obtain additional insights into their customers' connection speeds, ISPs, and more using GeoIP data.
- <https://www.maltego.com/transform-hub/maxmind/>
- <https://github.com/libresec/geo-ip-maltego>

Dark Web Investigation

- [Ahmia](#) – one of the oldest and most reliable .onion search engines, accessible both from the darknet and the clearnet.
- [Onion Search Engine](#) – for searching onion sites. It comes with browser extensions for Chrome and Firefox. Various supported search options include images, videos, maps and pastes.
- [Tor Taxi](#) – a launchpad website with links to multiple different onion domains. It has a handy colour-coded system for displaying websites that are currently down.
- [Darkweb Wiki](#) – a somewhat chaotic and not frequently updated list of onion sites – still, a valuable resource.
- [Hunchly](#) – provides daily darkweb reports of what onion domains are up / down, in the form of a spreadsheet.
- [IACA Darkweb Tools](#) – free resources provided by the International Anti Crime Academy.
- **Reddit communities** – many subreddits dedicated to various aspects of the darkweb can be found, some of which are hit and miss. However, there are 3 that are consistently good and up to date:
 - <https://www.reddit.com/r/darknet/>
 - <https://www.reddit.com/r/TOR/>
 - <https://www.reddit.com/r/onions/>
- **Discord** – an up-and-coming alternative to Reddit for budding online communities and niche topics, Discord already dominates in some aspects. While I have not yet found a publicly available channel worthy of a recommendation, you can darknet-keyword search the [available Discord servers](#).

Dark Web Investigation 2

- **Ahmia** – as mentioned above, but specifically for Tor:
- <http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion>
- **Haystak** – the self appointed “darknet’s largest search engine”, with thousands of indexed .onion domains – including some historical ones.
- <http://haystak5njsmn2hqkewecpaxetahtwhsbsa64jom2k22z5afxhnpxfid.onion/>
- **Kilos** – darknet market search engine allowing to search for vendors, listings, reviews, forums and forum posts. Useful for conducting broad keyword-based searches across multiple darkweb entities.
- <http://mlyusr6htlxsync7t2f4z53wdxh3win7q3qpxcrbam6jf3dmua7tnzuyd.onion/search>
- **TOR66** – on top of the standard search, this enables the “fresh onions” and “random onions” matches; tread with caution, these can bring you to some truly random sites.
- <http://tor66sewebgixwhcqfnp5inzp5x5uohhdy3kvtnyfxc2e5mxiuh34iid.onion/>

Dark Web Investigation 3

- First and foremost, awesome list of tools by Apurv Singh Gautam is available [here](#) (but just a caveat, I have not used or tested all of those – yet).
- [Onioff](#) – a Python tool for searching .onion URLs.
- [Onion Ingestor](#) – for scraping and collecting darkweb intelligence – works with Kibana dashboards.
- [Onion Search](#) – tool for scraping .onion URLs from darkweb search engines.
- [The Devils Eye](#) – for extracting .onion site links and descriptions without connecting to Tor.
- [TorBot](#) – onion crawler, with many additional features still in active development.

Dark Web Investigation 4

- [AuCyble](#)
- [DarkDotFail](#)
- [darktracer_int](#)
- [darkowlcyber](#)
- [ido_cohen2](#)
- [josephfcx](#)
- [RansomAlert](#)
- [Torproject](#)

Emails Analyzer

- Whenever an email is sent, information is transmitted with that email and the route the email takes across a network is recorded. This information is known as the 'Extended Header'.
- The extended header can be of great use to the researcher and when used correctly, provides an insight into the sender, their software and hardware and potential recipients.
- The extended header information potentially includes the senders IP address, email client, return address and the route the email has taken to reach its destination. This is useful in identifying and investigating 'spoof' or 'phishing' emails.

Emails Analyzer - Tools

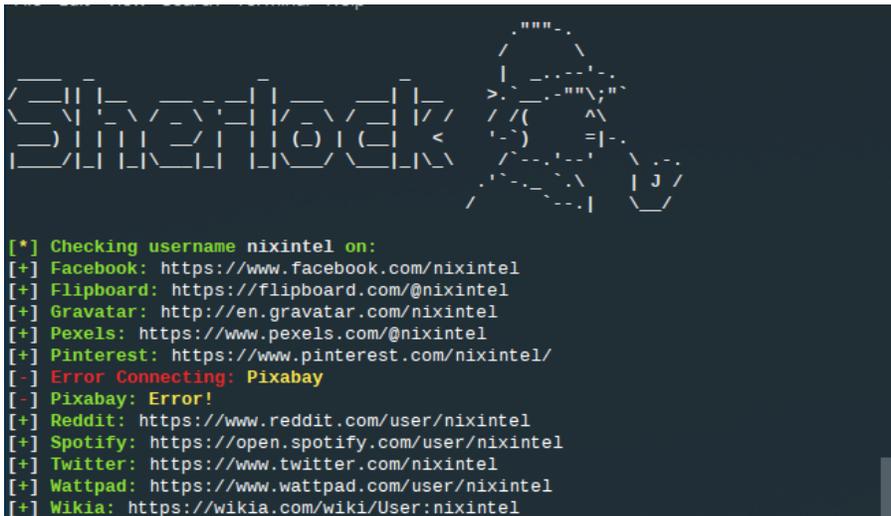
- Google Hacking;

site:organisation.com intext:@organisation.com

site:bbc.co.uk intext:@bbc.co.uk

intext:"boris.johnson.mp@parliament.uk" filetype:pdf

- Sherlock;



```
[*] Checking username nixintel on:  
[+] Facebook: https://www.facebook.com/nixintel  
[+] Flipboard: https://flipboard.com/@nixintel  
[+] Gravatar: http://en.gravatar.com/nixintel  
[+] Pexels: https://www.pexels.com/@nixintel  
[+] Pinterest: https://www.pinterest.com/nixintel/  
[-] Error Connecting: Pixabay  
[-] Pixabay: Error!  
[+] Reddit: https://www.reddit.com/user/nixintel  
[+] Spotify: https://open.spotify.com/user/nixintel  
[+] Twitter: https://www.twitter.com/nixintel  
[+] Wattpad: https://www.wattpad.com/user/nixintel  
[+] Wikia: https://wikia.com/wiki/User:nixintel
```

Emails Analyzer – Tools 2

- Pastebin;
- Have I been pwned?
- Emailrep.io;
- Hunter.io;
- Whitepages;
- Twitter;
- Mxtoolbox;
- Spiderfoot;
- ProtOsint;
- <https://github.com/bitsofinfo/comms-analyzer-toolbox>

Threat Intelligence Platform

- MISP;
- OpenCTI;
- IBM X-Force Exchange;
- ManageEngine;
- Anomali ThreatStream;
- LogRhythm TLM;
- Mandiant Threat Suite;
- Recorded Future;
- Virus Total Intelligence;
- Shodan;

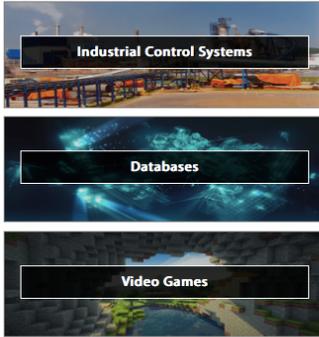
Shodan Malware Hunter

- <https://malware-hunter.shodan.io/>
- Malware Hunter is a specialized Shodan crawler that explores the Internet looking for command & control (C2s) servers for botnets. It does this by pretending to be an infected client that's reporting back to a C2. Since we don't know where the C2s are located the crawler effectively reports back to every IP on the Internet as if the target IP is a C2. If the crawler gets a positive response from the IP then we know that it's a C2.

Explore

Discover the Internet using search queries shared by other users.

Featured Categories



Top Voted

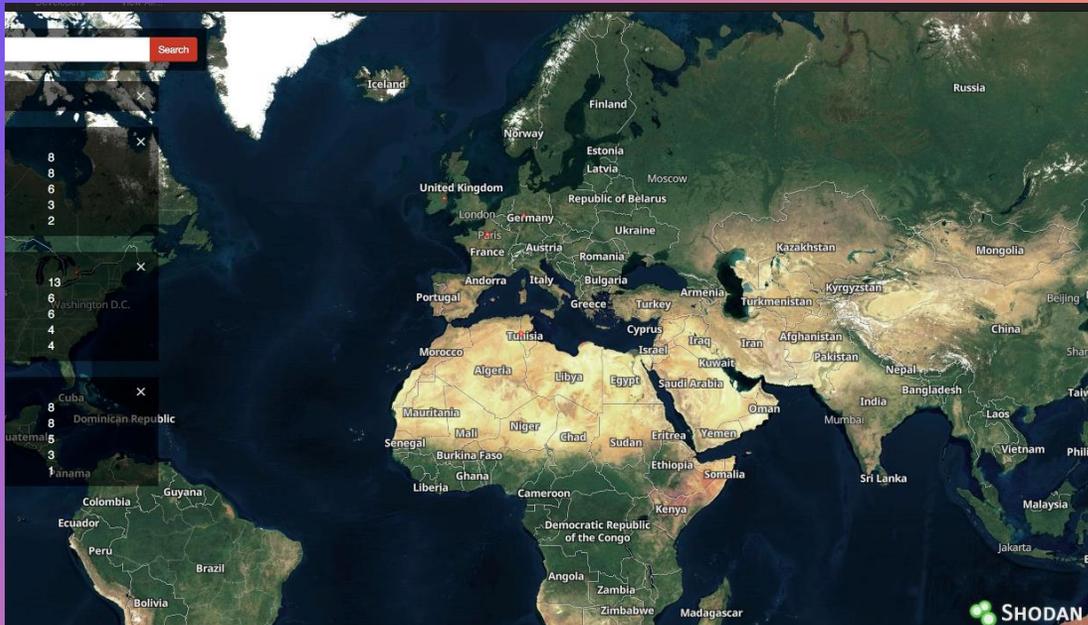
11,972	Webcam best ip cam search I have found yet. webcam surveillance cams 2010-03-15
4,957	Cams admin admin cam webcam 2012-02-06
2,575	Netcam Netcam netcam 2012-01-13
1,964	default password Finds results with "default password" in the ba... router default password 2010-01-14
1,238	WSO2 Carbon Servers

Recently Shared

1	1
1	NYPD NYPD nypd 2020-06-25
1	Netgear R6700v3
1	Argentina camaras 2020-06-25
1	WSO2 Carbon Servers

Shodan OSINT

- Shodan is a search engine that lets the user find specific types of computers (webcams, routers, servers, etc.) connected to the internet using a variety of filters. Some have also described it as a search engine of service banners, which are metadata that the server sends back to the client. This can be information about the server software, what options the service supports, a welcome message or anything else that the client can find out before interacting with the server.



SHODAN country:DE google port:80

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS
915

TOP COUNTRIES

Germany 915

TOP CITIES

Frankfurt am Main	155
Rastede	82
Berlin	38
Cologne	31
Münster	24

TOP ORGANIZATIONS

Versatel Deutschland	144
EWE-Tel GmbH	107
O2 Deutschland	93
Amazon.com	49
M-net	28

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

Error 404 (Not Found)!!1

62.214.82.49
cache.google.com
Versatel Deutschland
Added on 2020-06-26 08:25:39 GMT
Germany, Münster

```
HTTP/1.1 404 Not Found
Date: Fri, 26 Jun 2020 08:25:38 GMT
Content-Type: text/html; charset=UTF-8
Server: gvs 1.0
Content-Length: 1561
X-Google-Security-Signals: FRAMEWORK=HTTPSERVER2
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
```

Home Best Pal

35.207.124.154
154.124.207.35.bc.googleusercontent.com
Google Cloud
Added on 2020-06-26 09:49:51 GMT
Germany, Frankfurt am Main

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Fri, 26 Jun 2020 09:49:51 GMT
Content-Type: text/html
Content-Length: 259
Last-Modified: Tue, 23 Jul 2019 17:35:09 GMT
ETag: "5d37454d-103"
Accept-Ranges: bytes
Via: 1.1 google
```

ECB Statistical Data Warehouse

194.42.115.191
HTTP/1.1 200 OK

Shodan OSINT 2

- To select a specific country type: country: <Country Symbol>
- To select specific ports type: port: <Ports_HERE>
- To search for a specific operating system(OS) type: os: <OS_HERE>

SHODAN country:DE google

Exploits Maps Images Share Search Download Results Create Report

TOTAL RESULTS
4,728

TOP COUNTRIES

Germany 4,728

TOP CITIES

Frankfurt am Main	1,041
Berlin	234
Rastede	158
Nuremberg	148
Münster	36

TOP SERVICES

HTTPS	2,675
HTTP	915
8081	382
3001	89
8083	48

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

Error 404 (Not Found)!!1

212.53.171.254
Artfiles New Media GmbH
Added on 2020-06-26 10:54:21 GMT
Germany, Hamburg

SSL Certificate

Issued By:
- Common Name: GTS CA 101
- Organization: Google Trust
Services
Issued To:
- Common Name: *.googlevideo.com
- Organization: Google LLC

Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2, TLSv1.3

HTTP/1.1 404 Not Found
Date: Fri, 26 Jun 2020 10:54:20 GMT
Content-Type: text/html; charset=UTF-8
Server: gvs 1.0
Content-Length: 1561
X-Google-Security-Signals: FRAMEWORK=HTTPSERVER2
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN

217.160.157.231

finanzforum.biz
1&1 Internet AG
Added on 2020-06-26 10:50:43 GMT
Germany

```
HTTP/1.1 200 OK\r\nDate: Fri, 26 Jun 2020 10:50:43 GMT\r\nServer: Apache\r\nLast-Modified: Thu, 12 Apr 2012 15:04:11 GMT\r\n1950c0\r\nAccept-Ranges: bytes\r\nContent-Length: 3429\r\nContent-Type: text/html\r\n</FONT>\r\n</NOFRAMES>\r\n</B>\r\n<DOCTYPE HTML...
```

217.160.94.129

mail191807510.mywebspace.zone
1&1 Internet AG
Added on 2020-06-26 10:57:19 GMT
Germany

<https://www.bluetteamsacademy.com/shodan/>

Using Maltego to Identify and Investigate on C2 Malware in Your Network

- Maltego has a number of data integrations especially helpful for cybersecurity professionals and threat hunters seeking to identify hidden threats in the organization's network and trace the origin of said threats. In this tutorial, we will demonstrate how you can use Transforms from ATT&CK - MISP, VirusTotal Public API, and ZETAlytics Massive Passive to acquire threat intel, find hashes related to certain domains and IPs, and uncover threat actor network.
- Step 1: Identify Whether Hashes are False Alerts
- Step 2: Find Out Relevant IP Addresses using MISP Transforms
- Step 3: Investigate on Suspicious IP Addresses using ZETAlytics Transforms
- Step 4: Identify How the Malware Entered the Company Network
- Step 5: Deep-Dive into Malicious Domains to Find the Source of Malware Entry

<https://www.maltego.com/blog/identify-c2-malware-and-phishing-threats-with-maltego/>

Ransomware Playbook

The screenshot displays a digital playbook titled "Ransomware_Geno" with a green header. The interface is organized into several columns, each representing a phase of the incident response process. The "Playbook details" column on the left includes sections for "Playbook Source", "Internal Audit", "Controls/Compliance", and "Actions". The main flowchart consists of the following columns and cards:

- Preparation (4 cards):**
 - A1 - Identify and Document Defensive Measures Against Ransomware, the Alerts they Produce, and Tools that Can Be Used for Investigation
 - A2 - Identify and Document Ransomware Adversarial Playbook/TTPs/IOCs
 - A3 - Train Employees to Identify Ransomware Indicators and How to Report an Infection as Part of an Awareness Program
 - A4 - Build, Maintain, and Test Ransomware Prevention, Detection, Mitigation, and Response Capabilities - Fill Any Identified Gaps
 - A5 - Prepare Internal Stakeholders and External Resources (legal council, law enforcement, etc.) Prior to an Actual Event
 - A6 - Maintain Superior Security Hygiene (Patching, Backups, Access Control, etc.)
- Detect (9 cards):**
 - B1 - Threat Indicators/Alerts
 - B2 - Endpoint Security Solution Alert
 - B3 - User Reported Ransom Message
 - B4 - Unusual Quantity of Files Being Modified on Network Share(s) or Local Drives
 - B5 - Unusual CPU/Memory Utilization Alerts from Enterprise Monitoring Tools
 - B6 - Network Security Solution Alert, Ransomware Detection Rule, Unusual Web Browsing Activity (TOR, I2P Bitcoin Payment), Traffic On Known C2 Ports or To Known C2 Internet Hosts
 - B7 - User Reports Unusual Activity After Running an Executable File (VBS, Doc With Macro, JAR, PPT With Macro, etc.)
 - B8 - User Reports Files Not Available, Replaced With Known Ransomware File Extensions
 - B9 - User Reports Unusual Email With Attachment
- Triage (11 cards):**
 - C1 - Evaluate Loss Expectation
 - C2 - Probable Loss Magnitude Assessment
 - C3 - Reputation Damage
 - C4 - Fines/Judgements
 - C5 - Loss to Replace or Repair
 - C6 - Loss of Productivity
 - C7 - Loss Due to Legal Response
 - C8 - Loss of Competitive Advantage
 - C9 - Determine Severity Classification and Notification Requirements
 - C10 - Severity Assessment
 - C11 - Possibility of Data Compromise/Breach
- Analyze (8 cards):**
 - D1 - Positive ID from Indicators/Alerts?
If NO goto D2
If Yes goto D7
 - D2 - Gather Forensic Data (if needed)
 - D3 - Generate Hash From Suspect File & Send To Sandbox, AV Vendor, VirusTotal, etc. For ID
 - D4 - Lookup Other Gathered Indicators to Identify Ransomware Variant
 - D5 - Prior Known Variant ID is Not Possible, Perform Behavioral Analysis and Reverse Engineering. Skip if You Have an ID
 - D6 - Encryption Capabilities?
If NO Use Malicious Code Playbook
If Yes goto D7
 - D7 - Check Ransomware Census (goo.gl/b9R8DE) and Other Sources for Decryptor and Additional Indicators
 - D8 - Download an Authoritative Write-Up (if available) for the Specific Ransomware Variant(s) Encountered. Harvest Additional Indicators from the Report(s). (This report will also be used in the next phase to answer questions)
- Contain/Eradicate (8 cards):**
 - E1 - Able to blacklist executables?
If NO goto E3
If Yes goto E2
 - E2 - Blacklist Ransomware and Dropper/Infection/Persistence Mechanism Hashes. Goto E7
 - E3 - Scan Endpoints and Check System/Network Artifacts (Logs Flows, etc) for Indicators of Compromise and Lateral Movement
 - E4 - Does this Ransomware Variant Spread Itself?
If NO goto E7
If Yes goto E5
 - E5 - If Possible, Block Known Communication and Infection Channels (Firewall, Email Senders, NAC, etc.)
 - E6 - Isolate (disconnect wireless and wired) and Acquire Infected Hosts
 - E7 - Use Remotes (if available)/Admin Tools to Kill Malicious Processes and Remove Files/Persistence Mechanisms from Infected Hosts, or Re-image/Rebuild
 - E8 - Apply Patches, Security
- Post-Incident (6 cards):**
 - F1 - Incident Review
 - F2 - Review Lessons Learned
 - F3 - Review Lessons Applied
 - F4 - Evaluate Gaps In Prevention, Detection, Response, Remediation, Make Corrective Action Recommendations to Management
 - F5 - Update Documentation, Procedures, and Playbooks
 - F6 - Create, File, and Communicate Final Reports to Stakeholders
- License (1 card):**
 - This work is licensed under Creative Commons Attribution-ShareAlike 4.0 International License

<https://github.com/counteractive/incident-response-plan-template/blob/master/playbooks/playbook-ransomware.md>

References

- <https://www.trellix.com/en-us/security-awareness/ransomware/what-is-ransomware.html>
- <https://us.norton.com/internetsecurity-malware-types-of-ransomware.html>
- <https://h11dfs.com/9-step-ransomware-incident-response-plan/>
- <https://dxc.com/us/en/insights/perspectives/paper/ransomware-survival-guide---recover-from-an-attack->
- <https://www.sentinelone.com/cybersecurity-101/open-source-intelligence-osint/>
- https://www.researchgate.net/figure/Model-for-the-money-laundering-of-ransomware-and-cryptoware-profits-via-bitcoins_fig2_343009039
- <https://bitquery.io/blog/trace-bitcoin-transaction-and-address>
- <https://www.secjuice.com/osint-daily-dose-of-malware/>