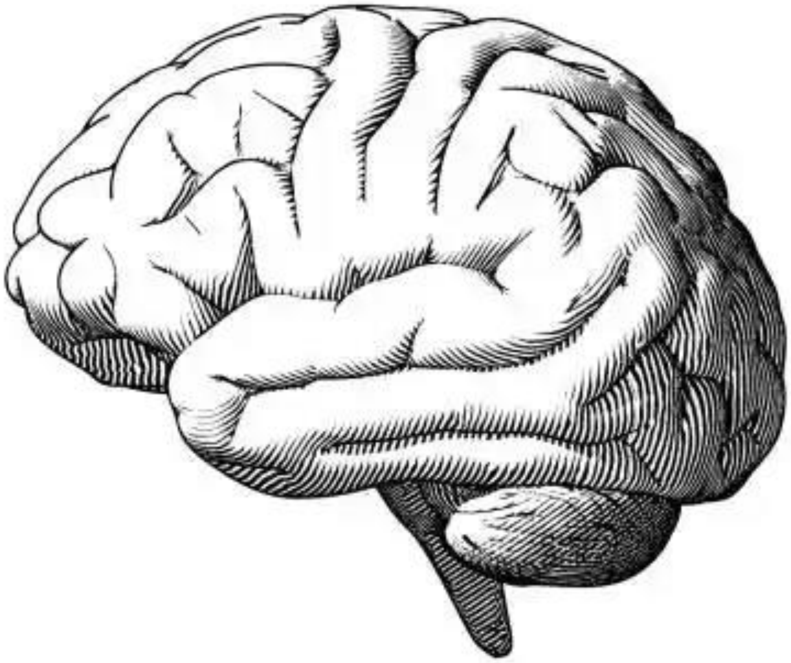


OSINT GATHERING & APPLICATION

Creating Actionable Open Source Intelligence in Cyber Security

Written by Daniel J. Conrad

INTRODUCTION

What is OSINT?

OSINT, or Open Source Intelligence, is freely available information that can be gathered from publicly accessible channels to be used specifically in the context of intelligence gathering. These publicly accessible channels can include internet sources, news broadcasts, public government data, or even academic publications.

As defined by the DOD, OSINT is intelligence that is "produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."

OSINT in Cyber Security

Cyber Security personnel can benefit greatly from OSINT collection and application. With no security tool, firewall, or IPS being perfect, actively gathering new intelligence for either immediate or future use can aid in an organization's ability to effectively combat incoming and distant threats.

Thankfully, due to the very definition of OSINT, gathering this intelligence does not require any special tools, expensive subscriptions, or extreme technical ability. The primary cost of this type of intelligence gathering is the analyst's time, since there are several steps that must be followed to ensure accurate and timely dispersion of information.

What You'll Need

The very few tools that you will need to utilize are listed below:

- A modern computer capable of accessing the internet.
- An active internet connection.
- A trusted browser such as Firefox or Brave.
- Documentation software such as Word or Open Office.
- The TOR Browser.
    - If you are unfamiliar with TOR or the TOR Browser, check the documentation.
- VPN – Not required, but *highly* recommended.

Table of Contents

Introduction

Basic OSINT Gathering

Verification

Documentation

Advanced OSINT Gathering

Potential Threat Reports

Conclusion

BASIC OSINT GATHERING

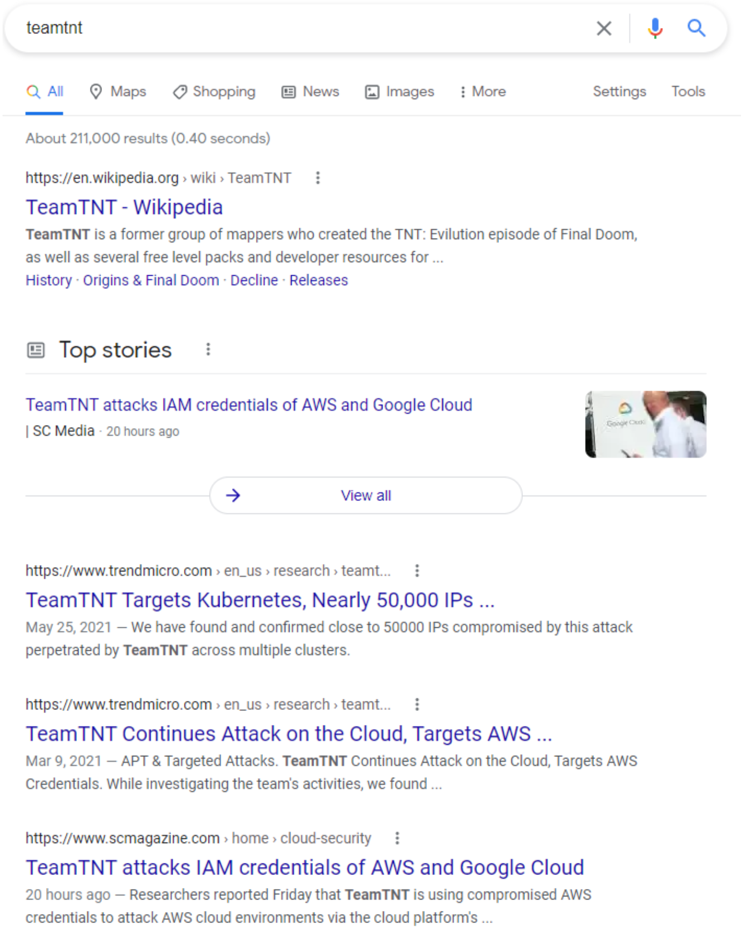
Searching for Known Threats

Assuming you have a modern computer and are connected to the internet, obtaining large amounts of information does not require much effort. Instead, there is so much information and "noise" that is found on the internet that the real work comes from filtering and utilizing common sense to find valuable information on active or future threats. When gathering OSINT, be sure to document your sources, and take screenshots of things that are either of interest or may be taken down / deleted at a later date.

Social media feeds such as Twitter are a fantastic place to stumble upon OSINT. However, with over 186 million Twitter users as of 2020, where does one begin to look? The same question is asked for sites such as PasteBin, a website that allows users to store plain text via public posts, and receives 17 million unique posts a month. Though initially created for programming and code review, it is often used for publicizing breached data, dark web links (we'll get to those later), and source code for both malicious and non-malicious applications. So the question remains: how is one supposed to sift through all of this noise? Thankfully, Google constantly crawls and indexes websites and posts just like those that we are looking for. By utilizing the search of "site:example.com your_search_here", we can greatly reduce the noise that is typically found when looking for OSINT.

In the following examples, we search for TeamTNT activity, a German-based threat group known for compromising cloud environments. Without using the "site:" function, we are greeted with many different articles, some being valuable, some not.

In the next screenshot, we apply our "site:" function to search through Twitter. One interesting fact that is not mentioned in the majority of articles is that TeamTNT utilizes social media for both self-promotion and taunting. This is why searching additional channels such as Twitter, PasteBin, or Reddit may be of additional value to your search.



teamtnt

About 211,000 results (0.40 seconds)

https://en.wikipedia.org › wiki › TeamTNT

TeamTNT - Wikipedia

TeamTNT is a former group of mappers who created the TNT: Evilution episode of Final Doom, as well as several free level packs and developer resources for ...

History · Origins & Final Doom · Decline · Releases

Top stories

TeamTNT attacks IAM credentials of AWS and Google Cloud

| SC Media · 20 hours ago

https://www.trendmicro.com › en_us › research › teamt...

TeamTNT Targets Kubernetes, Nearly 50,000 IPs ...

May 25, 2021 — We have found and confirmed close to 50000 IPs compromised by this attack perpetrated by **TeamTNT** across multiple clusters.

https://www.trendmicro.com › en_us › research › teamt...

TeamTNT Continues Attack on the Cloud, Targets AWS ...

Mar 9, 2021 — APT & Targeted Attacks. **TeamTNT** Continues Attack on the Cloud, Targets AWS Credentials. While investigating the team's activities, we found ...

https://www.scmagazine.com › home › cloud-security

TeamTNT attacks IAM credentials of AWS and Google Cloud

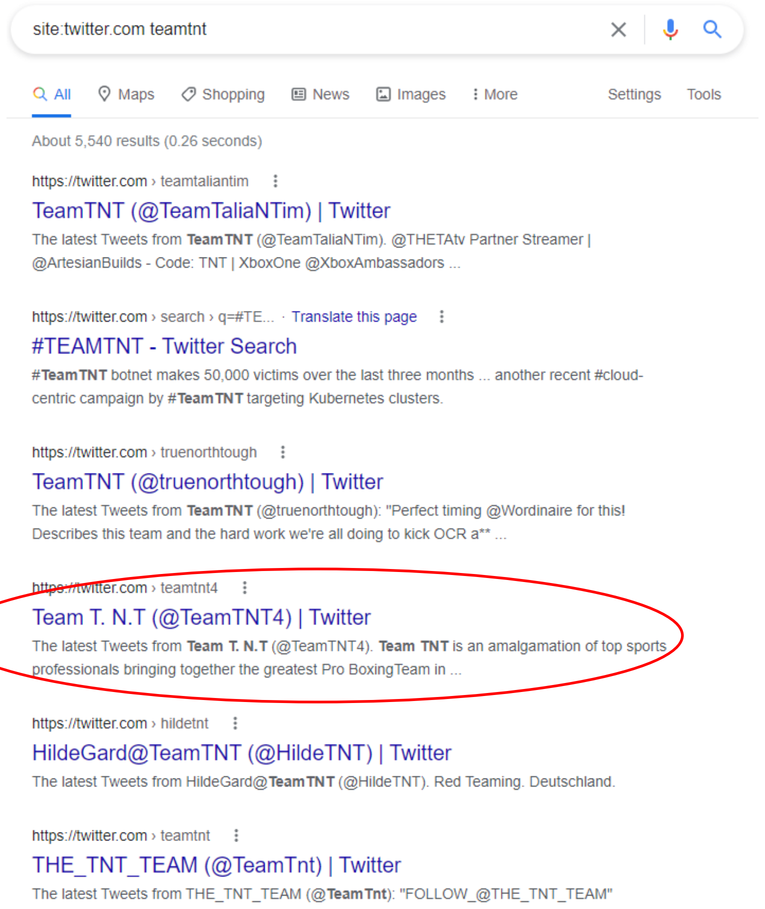
20 hours ago — Researchers reported Friday that **TeamTNT** is using compromised AWS credentials to attack AWS cloud environments via the cloud platform's ...

FIGURE 1 GOOGLE SEARCH FOR "TEAMTNT"

We can see that using the "site:" function for Twitter greatly narrowed the results to only show relevant information from Twitter regarding TeamTNT.

It is pretty straight forward to pick out which twitter account belongs to TeamTNT. Since we know they are a German-based threat, the obvious choice contains "Deutschland" in the biography, along with "Red Teaming".

After exploring the Twitter account in question, we quickly come to the realization that the majority of these tweets are in German. Google Translate does a fine job at translating these tweets into interpretable English, with the results listed below. It looks like TeamTNT doesn't plan on giving up any time soon. This would be a good feed to monitor in the future.



site:twitter.com teamtnt

About 5,540 results (0.26 seconds)

https://twitter.com › teamtaliantim
TeamTNT (@TeamTaliaNTim) | Twitter
The latest Tweets from **TeamTNT** (@TeamTaliaNTim). @THETAtv Partner Streamer | @ArtesianBuilds - Code: TNT | XboxOne @XboxAmbassadors ...

https://twitter.com › search › q=#TE... · Translate this page
#TEAMTNT - Twitter Search
#**TeamTNT** botnet makes 50,000 victims over the last three months ... another recent #cloud-centric campaign by #**TeamTNT** targeting Kubernetes clusters.

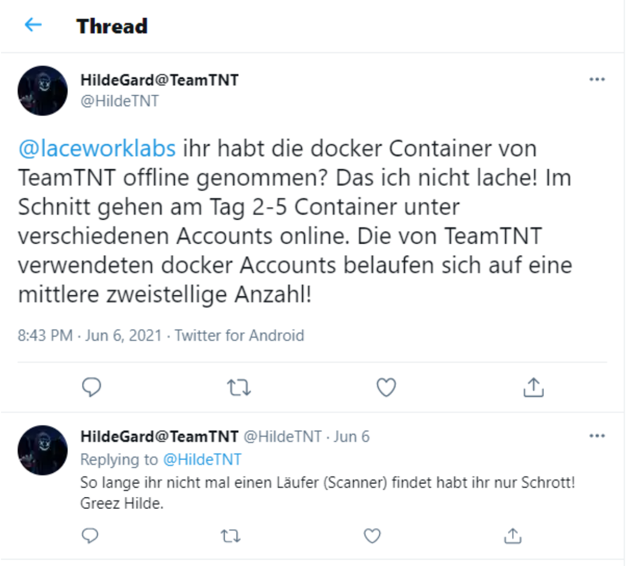
https://twitter.com › truenorthtough
TeamTNT (@truenorthtough) | Twitter
The latest Tweets from **TeamTNT** (@truenorthtough): "Perfect timing @Wordinaire for this! Describes this team and the hard work we're all doing to kick OCR a** ...

https://twitter.com › teamtnt4
Team T. N.T (@TeamTNT4) | Twitter
The latest Tweets from **Team T. N.T** (@TeamTNT4). **Team TNT** is an amalgamation of top sports professionals bringing together the greatest Pro BoxingTeam in ...

https://twitter.com › hildetnt
HildeGard@TeamTNT (@HildeTNT) | Twitter
The latest Tweets from HildeGard@**TeamTNT** (@HildeTNT). Red Teaming. Deutschland.

https://twitter.com › teamtnt
THE_TNT_TEAM (@TeamTnt) | Twitter
The latest Tweets from THE_TNT_TEAM (@**TeamTnt**): "FOLLOW_@THE_TNT_TEAM"

FIGURE 2 GOOGLE SEARCH UTILIZING "SITE:" TOOL



Thread

HildeGard@TeamTNT
@HildeTNT

@laceworklabs ihr habt die docker Container von TeamTNT offline genommen? Das ich nicht lache! Im Schnitt gehen am Tag 2-5 Container unter verschiedenen Accounts online. Die von TeamTNT verwendeten docker Accounts belaufen sich auf eine mittlere zweistellige Anzahl!

8:43 PM · Jun 6, 2021 · Twitter for Android

HildeGard@TeamTNT @HildeTNT · Jun 6
Replying to @HildeTNT
So lange ihr nicht mal einen Läufer (Scanner) findet habt ihr nur Schrott! Greez Hilde.

Translation (Approximate):

@laceworklabs you took the TeamTNT docker containers offline? That I don't laugh! On average, 2-5 containers go online under different accounts a day. The docker accounts used by TeamTNT amount to a middle double-digit number!

As long as you don't even find a runner (scanner) you only have scrap! Greez Hilde.

Searching for Unknown Threats

Aside from searching with Google to find information, we can rely on some trustworthy news sources to alert and identify threats. Even though we may trust the source from which the information is coming from, we still want to verify that it is correct in both what is provided and the fact that it is malicious. Below is a table of news sources and verification tools that can be used to help validate any gathered OSINT. This is not a complete or exhaustive list, just enough to get you started.

News Source	Link
Cyware	cyware.com/cyber-security-news-articles
Alien Vault	otx.alienvault.com
Krebs on Security	krebsonsecurity.com

Verification Source	Link
Virus Total	virustotal.com
Talos File Intelligence	talosintelligence.com/talos_file_reputation
AbuseIPDB	abuseipdb.com

At the time of writing, Cyware News is one of my all-time favorite news feeds. Posts are made regularly and are up-to-date with the current threat landscape. However, an article or two alone does not generate the kind of information we are looking for. After all, a news article is simply someone else's writing. It's great to have a trusted source for security updates and threat news, but we still need to verify the following:

1. The program / file in question is indeed malicious.
2. The IP address or addresses are abused and act maliciously.
3. The domain, URL, or hostname are malicious or have direct ties to malicious behavior.

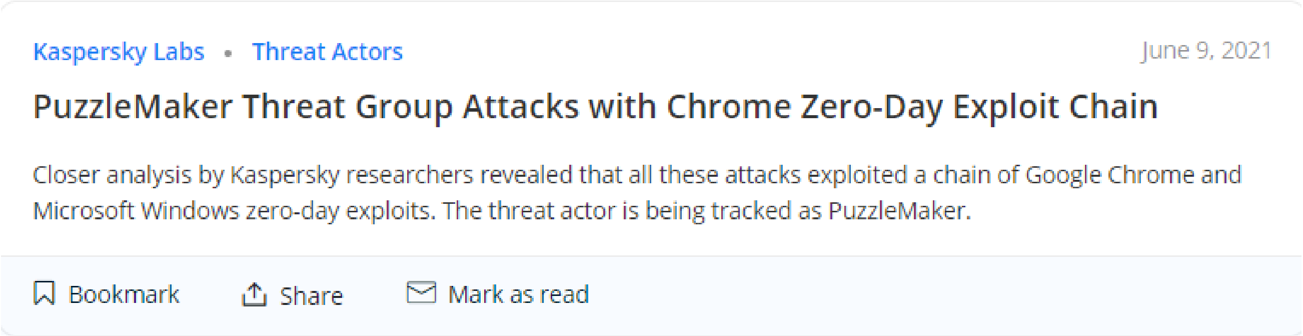
The aforementioned "to-do" list to verify a program or machine's behavior may vary depending on the type of threat you are looking into, derived from your news source. For example, a simple phishing scheme that directs users to a familiar-looking site to enter in their credentials (credential theft), may not need to utilize malicious programs to achieve its goal. It is important to understand the potential threat at hand, and analyze it accordingly.

An interesting note on looking into IP addresses – with the rapid rise of "cloud" IP's, and the ability to quickly shift, spoof, or otherwise change IP addresses, you may find many IP's that have been used maliciously, yet they are "whitelisted". This is usually due to the fact that a large company such as Google or AWS operates those IP addresses, however they are leased out to individuals, where the malicious behavior then occurs. There is also nothing stopping an attacker from spoofing their IP address again, so be cautious when basing any findings purely from IP addresses.

VERIFICATION

Example Search & Verification

In the example below, we will walk through searching for previously unknown threats with OSINT. We will also attempt to verify the findings utilizing some of the same tools mentioned in the previous section, such as Virus Total and Alien Vault. The verification process applies to both known and unknown threats – any file hash, IP, or domain must be verified and validated. We will start by looking at our news source, Cyware.



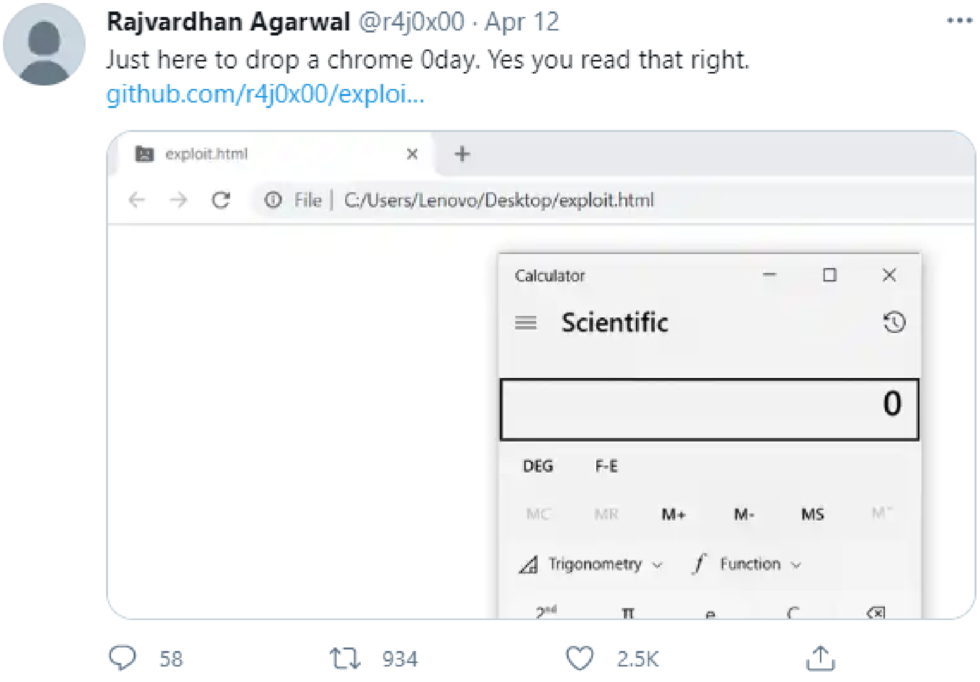
Kaspersky Labs • Threat Actors June 9, 2021

PuzzleMaker Threat Group Attacks with Chrome Zero-Day Exploit Chain

Closer analysis by Kaspersky researchers revealed that all these attacks exploited a chain of Google Chrome and Microsoft Windows zero-day exploits. The threat actor is being tracked as PuzzleMaker.

Our first article of interest is a Chrome Zero-Day exploit. The article itself contains some great information on what the alleged exploit does, and how it works. It also drops a Twitter handle for the exploit creator as well as their GitHub handle, so let's check those out. Keep in mind, creating an exploit of software isn't malicious in its own, the *application* of that exploit is.

To the right is the exploit developer's Twitter feed, along with the link to the exploit.

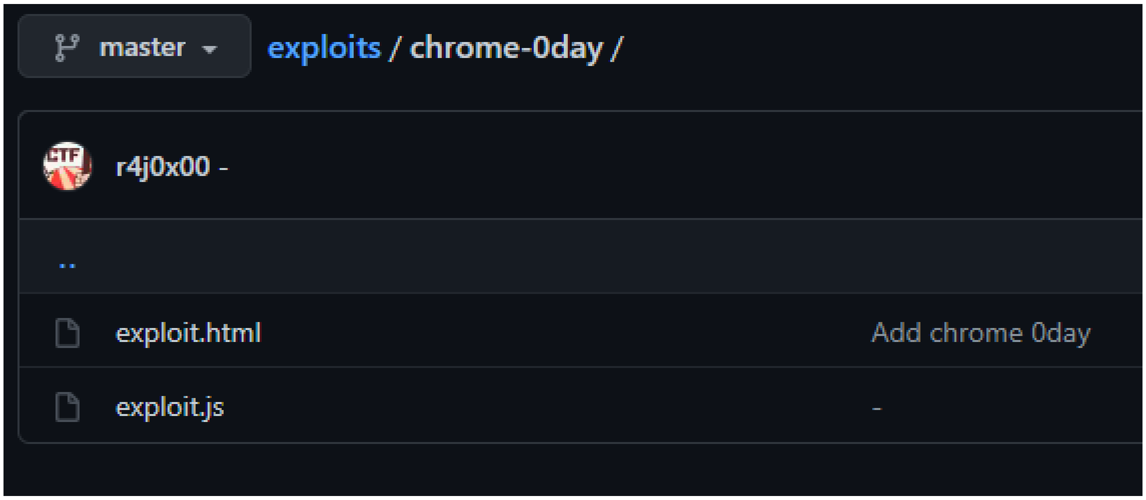


Rajvardhan Agarwal @r4j0x00 · Apr 12

Just here to drop a chrome 0day. Yes you read that right.
github.com/r4j0x00/exploi...

FIGURE 3 TWITTER RESULTS FOR @R4J0X00

By following the GitHub link, we can see that he has indeed placed two files of "exploit.html" and "exploit.js" in the chrome-0day repository. The Cyware article had informed us that this exploit is used to execute a remote shellcode in the context of the browser renderer process. Without diving too much deeper in to the technicalities of the exploit, we need to find some actionable Indicators of Compromise (IOC's) to verify.



master ▾ exploits / chrome-0day /

r4j0x00 -

..

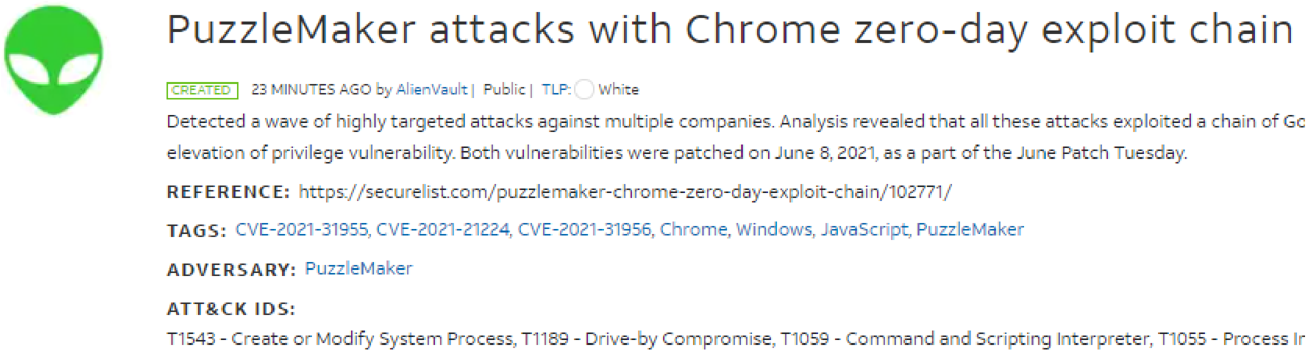
exploit.html Add chrome 0day

exploit.js -

FIGURE 4 GITHUB RESULTS: R4J0X00

Some articles are kind enough to include the sought-after IOC's, while some are not. Alien Vault is very helpful in identifying these for further verification if the article has not included them. Utilizing Alien Vault's search engine for the keyword "puzzlemaker", we can quickly identify the file hashes and domains that are in question.

We are also able to see what sources they are pulling from, the CVE indicators, as well as MITRE ATT&CK ID's. These can all be used later to create a more complete picture of the exploit, but for now we simply want to gather as much accurate information on it as possible.



PuzzleMaker attacks with Chrome zero-day exploit chain

CREATED 23 MINUTES AGO by AlienVault | Public | TLP: ○ White

Detected a wave of highly targeted attacks against multiple companies. Analysis revealed that all these attacks exploited a chain of Gc
elevation of privilege vulnerability. Both vulnerabilities were patched on June 8, 2021, as a part of the June Patch Tuesday.

REFERENCE: https://securelist.com/puzzlemaker-chrome-zero-day-exploit-chain/102771/

TAGS: CVE-2021-31955, CVE-2021-21224, CVE-2021-31956, Chrome, Windows, JavaScript, PuzzleMaker

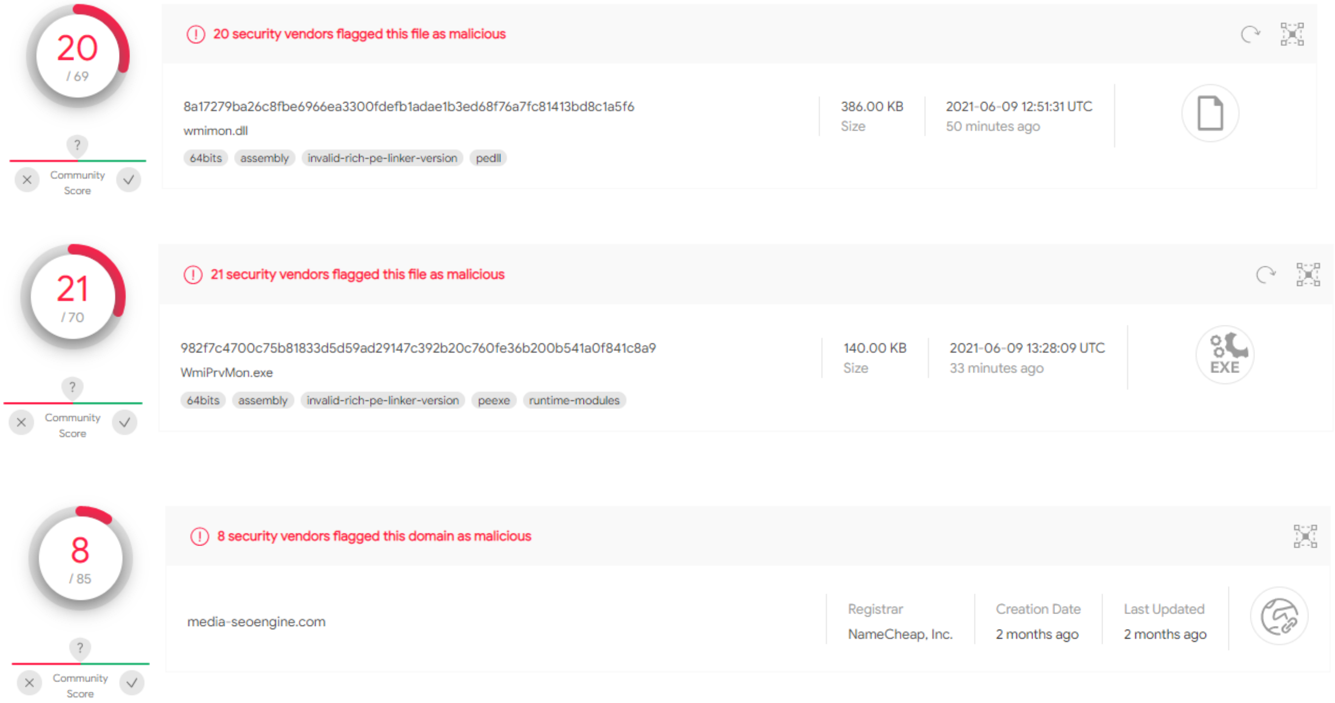
ADVERSARY: PuzzleMaker

ATT&CK IDS:

T1543 - Create or Modify System Process, T1189 - Drive-by Compromise, T1059 - Command and Scripting Interpreter, T1055 - Process Ir

FIGURE 5 ALIEN VAULT RESULTS

Now that we've identified the current IOC's for this exploit, we need to verify them. The reason behind verifying these is to validate your OSINT, especially since false positives and human error can occur. By placing these hashes and domains into Virus Total, we have the following output:



20 security vendors flagged this file as malicious

8a17279ba26c8fbe6966ea3300fdefb1adae1b3ed68f76a7fc81413bd8c1a5f6
wmimon.dll
64bits assembly invalid-rich-pe-linker-version pedll

386.00 KB
Size

2021-06-09 12:51:31 UTC
50 minutes ago

21 security vendors flagged this file as malicious

982f7c4700c75b81833d5d59ad29147c392b20c760fe36b200b541a0f841c8a9
WmiPrvMon.exe
64bits assembly invalid-rich-pe-linker-version peexe runtime-modules

140.00 KB
Size

2021-06-09 13:28:09 UTC
33 minutes ago

8 security vendors flagged this domain as malicious

media-seoengine.com

Registrar
NameCheap, Inc.

Creation Date
2 months ago

Last Updated
2 months ago

FIGURE 6-8 VIRUS TOTAL RESULTS

With a considerable amount of reputable security vendors reporting these files / domain to be malicious, we have successfully validated the IOC's that we found in Alien Vault. Now we must document our findings in such a way that is compelling and accurate to the knowledge we have.

The next section will cover documentation on OSINT, and walk through some simple practices you can apply to help keep your document clean, concise, and avoid rabbit holes. Clear documentation of your findings is key to successfully dispersing OSINT to the correct channels. It tells the right folks what they should consider blocking or monitoring, and a well-presented document can also add validity to your report, as opposed to a thrown-together glob of text.

DOCUMENTATION

Key Elements

OSINT documents can contain a lot of information. It can be challenging to break that information up into digestible bits for the appropriate channels, so utilizing an outline will be of benefit to you and your organization. Below is an example outline that can be tailored to fit your specific organizational needs.

I. **Executive Summary**
   a. Give the bottom line up front. In a paragraph, summarize the highlights of the OSINT, and the most important aspects of the information.
   b. Include a helpful chart or graph if the information is readily available. This can help convey your information, especially for non-technical individuals.

II. **Adversarial Information & Targets**
   a. If available, find information on the threat actor along with what organization or industry is being targeted. Not all threats have a specific target, and the adversary may not be known at the current time. If unknown, skip this section.

III. **Threat Information**
   a. Here, you can be more detailed in your findings of how the threat behaves, and what it does. You can utilize someone else's explanation if available, just be sure to cite it in your sources list.

IV. **Supplemental Information**
   a. This is for additional information such as graphs, charts, screenshots, or anything that helps others understand the threat at hand. Having this section of images may be valuable later, if you need to create a slideshow to present your findings to your management or leadership.

V. **Sources**
   a. Cite all articles or images that you've used. Inline citation such as "example [1]" is very helpful in showing where you found each piece of information from. Simply number your sources in the source list, and the inline citations will be a breeze.

In addition, it's a good idea to export your document to a PDF before sending it out. This makes the appearance of your OSINT more credible, and helps prevent others from easily modifying or changing your work.

On the next page is an example OSINT document that uses the aforementioned outline. For the sake of clarity, we will use the information that we found when investigating the Chrome Zero-Day Exploit.

OSINT Report – Chrome Zero-Day Exploit

By Daniel Conrad, June 9, 2021

Executive Summary

A zero-day exploit chain for Chrome was utilized on or around April 14, 2021 for remote code execution and privilege escalation by the threat actor "PuzzleMaker" against multiple companies, however no industries have been specified [1]. An official patch was released for both Chrome and Windows on June 8, 2021 [2], it is critical that Example Company machines be updated immediately to the latest versions of Chrome and Windows in order to mitigate this threat.

Adversarial Information & Targets

Adversary: PuzzleMaker [2]

Targeted Industries: Unknown

Threat Information

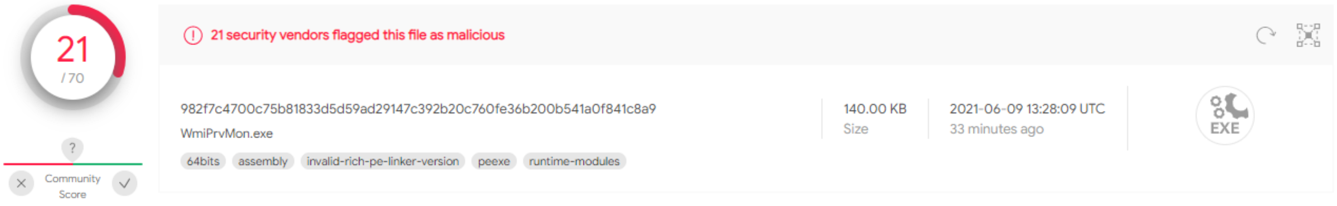
All IOC's - https://otx.alienvault.com/pulse/60c088d3fd6e59ee86c1b78b

Multiple zero-day exploits have been utilized in a chain-like fashion in order to compromise vulnerable machines, utilizing privilege escalation and executing remote code. The original exploit can be found on GitHub & Twitter [4] [5], along with the exploit author. The attack vectors of these exploits are below:

MITRE ATT&CK ID	DEFINITION
T1543	Create or Modify System Process
T1189	Drive-by Compromise
T1059	Command and Scripting Interpreter
T1055	Process Injection
T1134	Access Token Manipulation
T1057	Process Discovery
T1203	Exploitation for Client Execution
T1215	Kernel Modules and Extensions

Supplemental Information

Virus Total Findings [3]:



21 security vendors flagged this file as malicious

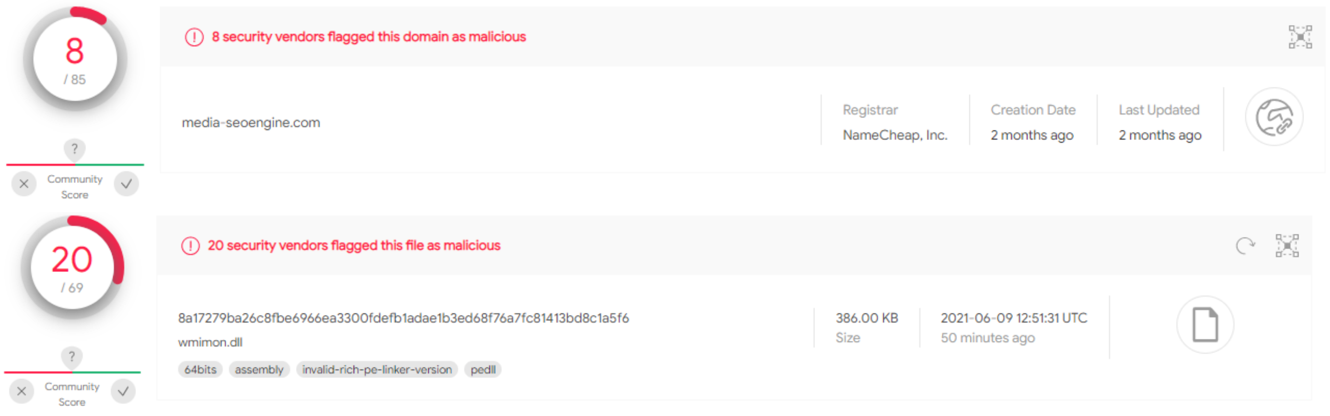
982f7c4700c75b81833d5d59ad29147c392b20c760fe36b200b541a0f841c8a9

WmiPrvMon.exe

140.00 KB Size

2021-06-09 13:28:09 UTC 33 minutes ago

Supplemental Information (Cont.)



8 / 85

Community Score

8 security vendors flagged this domain as malicious

media-seoengine.com

Registrar	Creation Date	Last Updated
NameCheap, Inc.	2 months ago	2 months ago

20 / 69

Community Score

20 security vendors flagged this file as malicious

8a17279ba26c8fbe6966ea3300fdefb1adae1b3ed68f76a7fc81413bd8c1a5f6

wmimon.dll

64bits assembly invalid-rich-pe-linker-version pedll

386.00 KB
Size

2021-06-09 12:51:31 UTC
50 minutes ago

Sources

[1]https://securelist.com/puzzlemaker-chrome-zero-day-exploit-chain/102771/?web_view=true

[2]https://otx.alienvault.com/pulse/60c088d3fd6e59ee86c1b78b

[3]https://www.virustotal.com/gui/file/982f7c4700c75b81833d5d59ad29147c392b20c760fe36b200b541a0f841c8a9/detection

[4] https://twitter.com/r4j0x00

[5] https://github.com/r4j0x00

The report above is not exhaustive, and to some degree it cannot be. This is open-source information, after all. This is what is freely available to the public over a common internet connection. OSINT does not include information that is gathered outside of public reach.

In the next section, we will begin discussing some more advanced ways to gather OSINT, making use of the TOR browser and some various Onion links.

Before continuing, you should feel comfortable doing the following:

1. Receive alerts through news sources on potential threats.
2. Research social media feeds for threat sources or additional information.
3. Find known IOC's for verification.
4. Verify IOC's via Virus Total, Talos File Intelligence, or another platform.
5. Clearly document your findings in an easy-to-read manner.

ADVANCED OSINT GATHERING

Setup

Gathering OSINT through other channels such as the TOR network can be of great value. Threats found on the TOR network are generally not public knowledge at the time but are still publicly accessible. However, it is not uncommon for many potential threats to materialize or become "the big bad wolf". Instead, utilize TOR findings to stay ahead of the threat, and to keep an eye on what is popular in hacking or malware-author communities.

I recommend the following when utilizing the TOR Browser:

1. Use a VPN, with the highest obfuscation settings.
2. Do not download or run programs found in TOR, unless you are on a dedicated machine and network that you are willing to have compromised.
3. When the TOR Browser is first launched, change the Security settings to "Safest". This disables all JavaScript that would normally run when you visit a TOR site.
4. Do not randomly click on links or ads. Be vigilant.
5. Utilize the "New Identity" function before and after your session.

I do not condone any illegal, immoral, or otherwise malicious behavior when utilizing the TOR browser. You alone are responsible for your actions and for the sites that you choose to visit. I will not advertise Onion links, they can be found in a variety of other manners, including on the regular internet as most know it (clearnet).

Searching in TOR

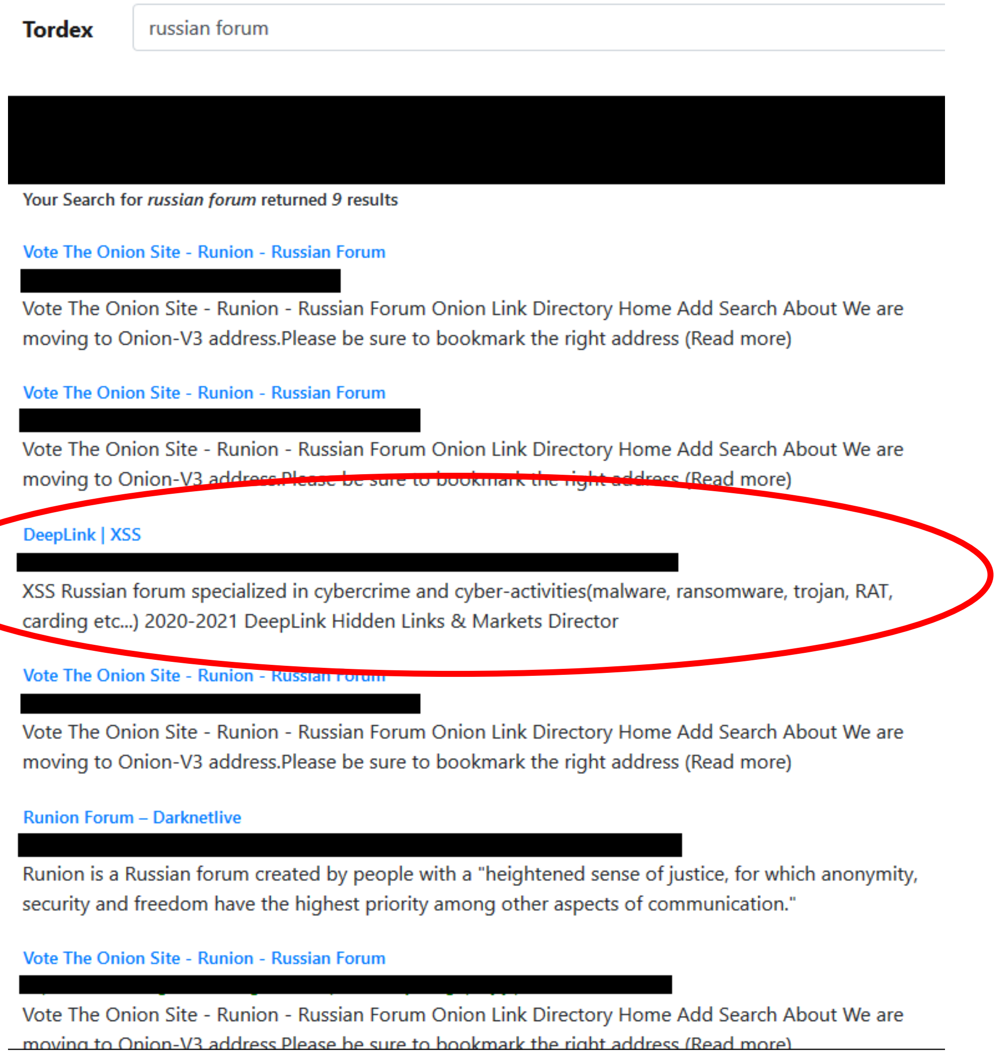
Searching in TOR is a bit different than searching in the clearnet. There is no Google. There are some different search index tools, but none of them come close to Google, Bing, etc. However, **Tordex** is a search index that I have found to be decent.

The primary goal of utilizing a search index is to find valuable forums, where potential threats may begin to develop, or new exploits are posted. A couple of forums that are great to stay on top of are below:

- **Dread** – Similar to Reddit with the idea of "subreddits" for various categories such as OPSEC, Drugs, Hacking, Malware, etc. Some threat groups can get started here and move to Telegram or another private messaging service, though users are generally weary of Law Enforcement (LE) interaction.
- **XSS.is** – Popular Russian language-based hacking forum. Includes a lot of exploits, malware development, and general vulnerability punishment.

Example TOR Search

Starting at Tordex, let us have a look for the infamous "Russian Hacking Forum" that everyone seems to have heard about. Without knowing that it the source is XSS.is, we will search for a generic keyword of "russian forum".



Tordex russian forum

[redacted]

Your Search for *russian forum* returned *9* results

Vote The Onion Site - Runion - Russian Forum

[redacted]

Vote The Onion Site - Runion - Russian Forum Onion Link Directory Home Add Search About We are moving to Onion-V3 address.Please be sure to bookmark the right address (Read more)

Vote The Onion Site - Runion - Russian Forum

[redacted]

Vote The Onion Site - Runion - Russian Forum Onion Link Directory Home Add Search About We are moving to Onion-V3 address.Please be sure to bookmark the right address (Read more)

DeepLink | XSS

[redacted]

XSS Russian forum specialized in cybercrime and cyber-activities(malware, ransomware, trojan, RAT, carding etc...) 2020-2021 DeepLink Hidden Links & Markets Director

Vote The Onion Site - Runion - Russian Forum

[redacted]

Vote The Onion Site - Runion - Russian Forum Onion Link Directory Home Add Search About We are moving to Onion-V3 address.Please be sure to bookmark the right address (Read more)

Runion Forum – Darknetlive

[redacted]

Runion is a Russian forum created by people with a "heightened sense of justice, for which anonymity, security and freedom have the highest priority among other aspects of communication."

Vote The Onion Site - Runion - Russian Forum

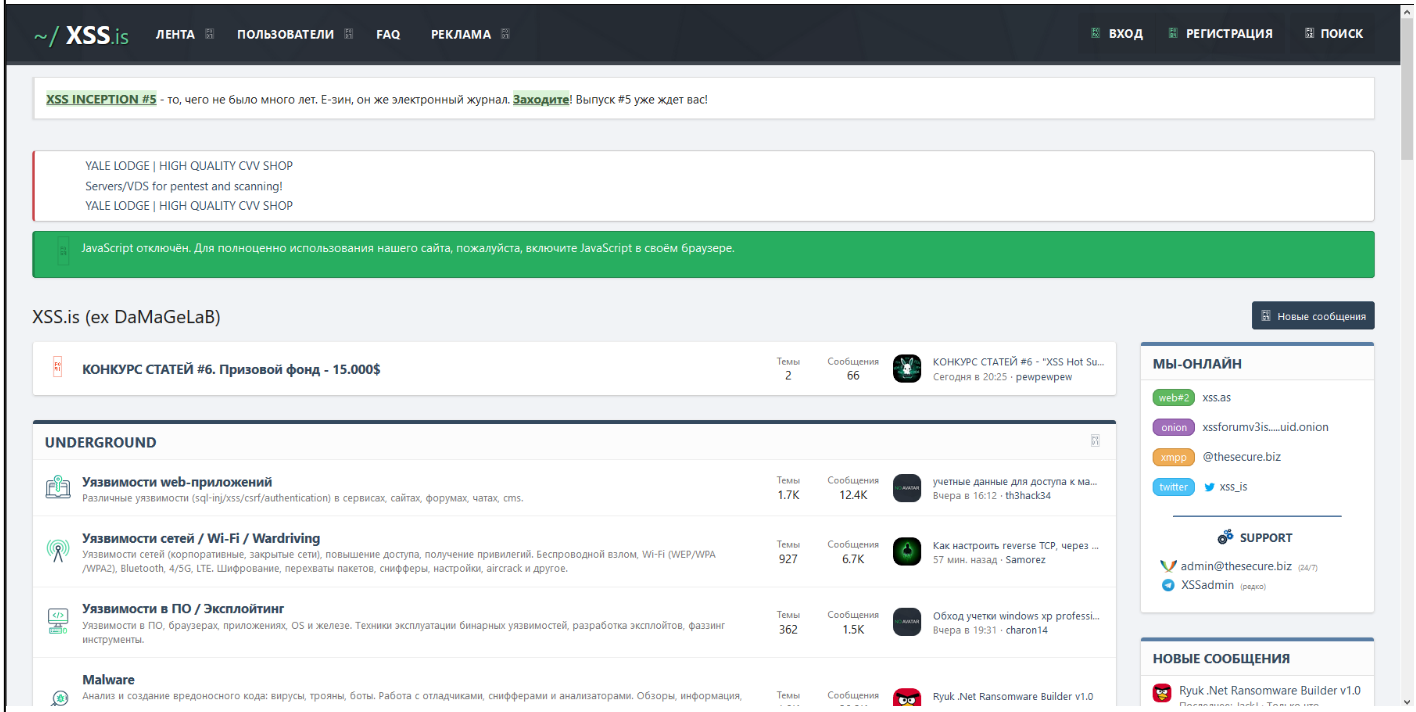
[redacted]

Vote The Onion Site - Runion - Russian Forum Onion Link Directory Home Add Search About We are moving to Onion-V3 address.Please be sure to bookmark the right address (Read more)

FIGURE 9 TORDEX RESULTS

DeepLink, along with many other TOR sites, is a link-list site. Link-lists are helpful in finding forums and other websites on the TOR network. They often display whether the website is currently running or is down. It is not uncommon for TOR websites to go down or offline, since they are maintained by small groups or individuals. Federal agencies have been known to have the ability take certain sites offline, or the site owners will take their site down to go into temporary hiding, only to reappear later with a different TOR link.

Following the DeepLink site, we come upon the Onion link for the Russian hacking forum, XSS.is. Below is a screenshot of what we find upon initial connection.



~/ XSS.is ЛЕНТА ПОЛЬЗОВАТЕЛИ FAQ РЕКЛАМА ВХОД РЕГИСТРАЦИЯ ПОИСК

XSS INCEPTION #5 - то, чего не было много лет. Е-зин, он же электронный журнал. Заходите! Выпуск #5 уже ждет вас!

YALE LODGE | HIGH QUALITY CVV SHOP
Servers/VDS for pentest and scanning!
YALE LODGE | HIGH QUALITY CVV SHOP

JavaScript отключён. Для полноценно использования нашего сайта, пожалуйста, включите JavaScript в своём браузере.

XSS.is (ex DaMaGeLaB)

Новые сообщения

КОНКУРС СТАТЕЙ #6. Призовой фонд - 15.000$ — Темы 2 — Сообщения 66 — КОНКУРС СТАТЕЙ #6 - "XSS Hot Su... Сегодня в 20:25 · pewpewpew

UNDERGROUND

Уязвимости web-приложений
Различные уязвимости (sql-inj/xss/csrf/authentication) в сервисах, сайтах, форумах, чатах, cms.
Темы 1.7K — Сообщения 12.4K — учетные данные для доступа к ма... Вчера в 16:12 · th3hack34

Уязвимости сетей / Wi-Fi / Wardriving
Уязвимости сетей (корпоративные, закрытые сети), повышение доступа, получение привилегий. Беспроводной взлом, Wi-Fi (WEP/WPA /WPA2), Bluetooth, 4/5G, LTE. Шифрование, перехваты пакетов, снифферы, настройки, aircrack и другое.
Темы 927 — Сообщения 6.7K — Как настроить reverse TCP, через ... 57 мин. назад · Samorez

Уязвимости в ПО / Эксплойтинг
Уязвимости в ПО, браузерах, приложениях, OS и железе. Техники эксплуатации бинарных уязвимостей, разработка эксплойтов, фаззинг инструменты.
Темы 362 — Сообщения 1.5K — Обход учетки windows xp professi... Вчера в 19:31 · charon14

Malware
Анализ и создание вредоносного кода: вирусы, трояны, боты. Работа с отладчиками, снифферами и анализаторами. Обзоры, информация,
Темы — Сообщения — Ryuk .Net Ransomware Builder v1.0

МЫ-ОНЛАЙН
web#2 xss.as
onion xssforumv3is.....uid.onion
xmpp @thesecure.biz
twitter xss_is

SUPPORT
admin@thesecure.biz (24/7)
XSSadmin (редко)

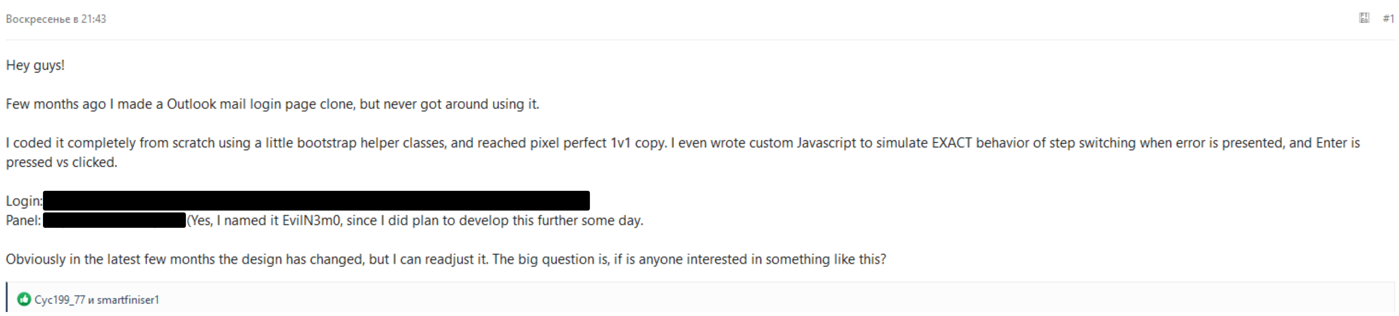
НОВЫЕ СООБЩЕНИЯ
Ryuk .Net Ransomware Builder v1.0

FIGURE 10 XSS.IS RESULTS

To roughly translate the forum sections found under the "Underground" section in the image above, including sections not listed in the image, are as follows:

- Vulnerabilities in Web Applications
- Network / Wi-Fi / Wardriving Vulnerabilities
- Software Vulnerabilities / Exploitation
- Malware (listed in English)
- Messengers and Social Networks
- Hardware Hacking & Phreaking (Phone System Hacking)
- Cryptography
- Anonymity and Security (OPSEC)
- Spam, Traffic, & Downloads
- SI / Phishing / APT (Advanced Persistent Threat) / Fraud

All forum channels listed above can be of value, depending on your organization. For this example, we will visit a recent English-post in the APT category. The image on the next page displays the forum post and its content.



Воскресенье в 21:43 #1

Hey guys!

Few months ago I made a Outlook mail login page clone, but never got around using it.

I coded it completely from scratch using a little bootstrap helper classes, and reached pixel perfect 1v1 copy. I even wrote custom Javascript to simulate EXACT behavior of step switching when error is presented, and Enter is pressed vs clicked.

Login: [redacted]
Panel: [redacted](Yes, I named it EvilN3m0, since I did plan to develop this further some day.

Obviously in the latest few months the design has changed, but I can readjust it. The big question is, if is anyone interested in something like this?

Cyc199_77 и smartfiniser1

FIGURE 11 XSS.IS FORUM POST

XSS.is Forum Post:

Hey guys!

Few months ago I made a Outlook mail login page clone, but never got around to using it.

I coded it completely from scratch using a little bootstrap helper classes, and reached pixel perfect 1v1 copy. I even wrote custom Javascript to simulate EXACT behavior of step switching when error is presented, and Enter is pressed vs clicked.

Login: <redacted>
Panel: <redacted> (Yes, I named it EvilN3m0, since I did plan to develop this further some day.

Obviously in the latest few months the design has changed, but I can readjust it. The big question is, if is anyone interested in something like this?

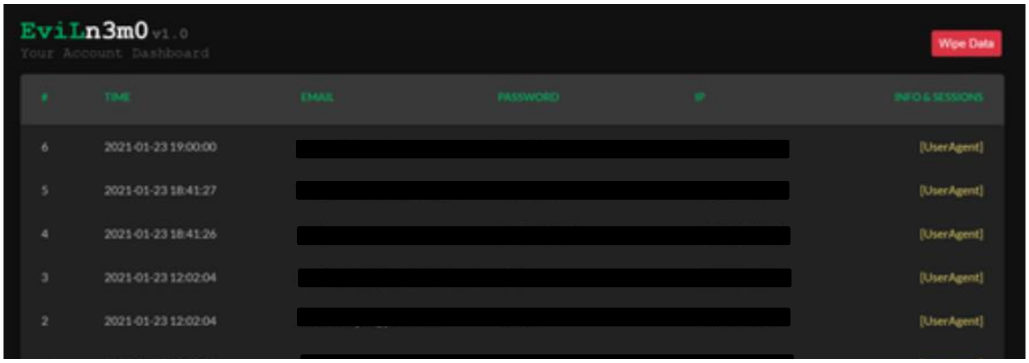
XSS User Reply:

YES DO IT

XSS User Reply:

Agreed, definitely do it

The account dashboard panel shown below is pulled directly from the "Panel" link that is displayed in the forum post:



#	TIME	EMAIL	PASSWORD	IP	INFO & SESSIONS
6	2021-01-23 19:00:00	[redacted]	[redacted]	[redacted]	[UserAgent]
5	2021-01-23 18:41:27	[redacted]	[redacted]	[redacted]	[UserAgent]
4	2021-01-23 18:41:26	[redacted]	[redacted]	[redacted]	[UserAgent]
3	2021-01-23 12:02:04	[redacted]	[redacted]	[redacted]	[UserAgent]
2	2021-01-23 12:02:04	[redacted]	[redacted]	[redacted]	[UserAgent]

FIGURE 11 EVILN3M0 DEMO

As seen above, the forum thread continues with other users encouraging the author to deploy the page for malicious use, and displays the attacker's view of IP addresses, email addresses, and passwords. The question remains, what information can we gather from this? How are we to present this information to supervisors and leadership about the potential threat?

From the above post, we can call this threat "EvilN3m0", and label it as a credential stealer, since it actively scrapes Outlook users' email addresses and passwords. However, we are at a standstill since we have no IOC's to actively apply to any security tools, as this threat is not yet released and has no active domains or URL's to study. Instead, we can create a Potential Threat Report, and escalate these documents to supervisors or leadership, or place them in a threat database, depending on your organization's standard operation procedures.

On the next page, we will create a Potential Threat Report based on our previous findings on EvilN3m0, an Outlook credential stealer that may or may not materialize into a threat at some point in the future.

POTENTIAL THREAT REPORTS

Key Elements

In this example, we will create a Potential Threat Report on the Outlook credential stealer, EvilN3m0. This report will not be as in-depth as a traditional OSINT report, since we cannot include indicators of compromise. Below is an example outline that can be tailored to fit your specific organizational needs.

I. **Executive Summary**
   a. Similarly, to the traditional OSINT reports, summarize the important aspects of the information on the potential threat. What does the threat do? How can your organization effectively combat this potential threat?

II. **Potential Threat Details**
   a. Explain how the potential threat works. Is it a simple credential-theft page that appears to be legitimate? Be detailed.

III. **Supplemental Information**
   a. If you can find more information on the potential threat or are experienced with metrics and programs like Pandas, Power BI, or similar, generate your own graphs & charts to help convey the potential threat. If one is particularly concise, place it in the Executive Summary.
   b. Include screenshots and or translations of the website that you found the potential threat on.

IV. **Sources**
   a. Add the title of the website and the Onion link that you found. Note, you should swap any “t” characters for “x” characters in “http”, resulting in “hxxp”. The reason behind this is nullifying the link, and if security tools prefetch links, you do not want them to flag an email as malicious when it contains valuable information. This is well known to the security community, so do not fear the swap!

Potential Threat Report – EvilN3m0

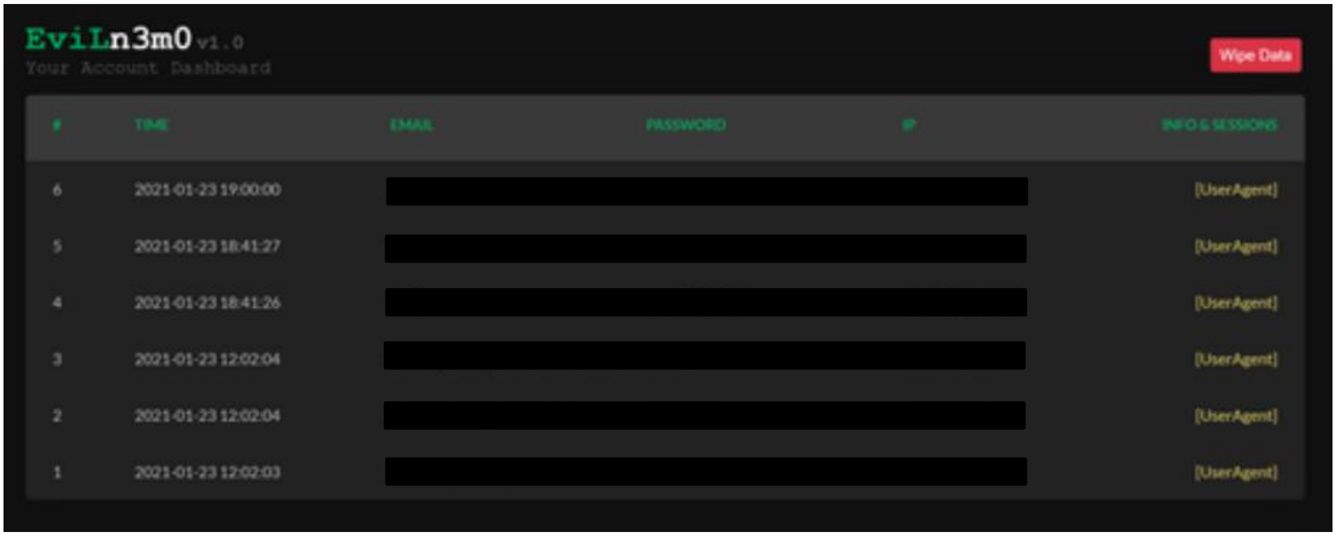
By Daniel Conrad, June 9, 2021

Executive Summary

EvilN3m0 appears to be a phishing website that has not yet been deployed. It operates by tricking the user into believing that they are entering their credentials into a trusted Microsoft Outlook website, when really, the credentials are stolen and given to the attacker. The best course of mitigation for this potential threat is to ensure users are aware of phishing emails and links, as well as utilize two-factor authentication to prevent password breaches. Users should also be trained on password security, and never utilize the same password twice.

Potential Threat Details

EvilN3m0 was discovered on XSS.is, a TOR-based website. XSS.is is a Russian-language based forum for hacking, exploit development, and malware creation. EvilN3m0 operates by spoofing the Microsoft Outlook login webpage, where users enter their credentials [1]. The credentials and IP addresses are then stolen and displayed to the attacker via the following portal:

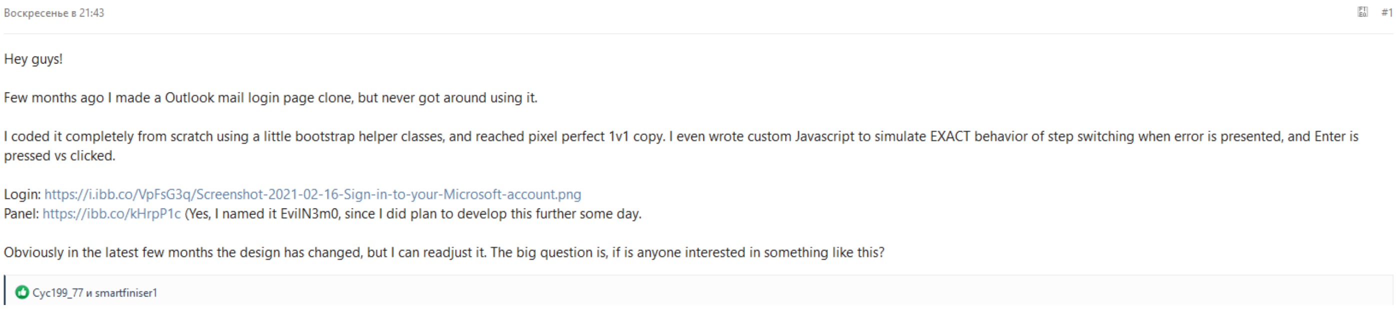


EviLn3m0 v1.0
Your Account Dashboard

#	TIME	EMAIL	PASSWORD	IP	INFO & SESSIONS
6	2021-01-23 19:00:00	[redacted]	[redacted]	[redacted]	[UserAgent]
5	2021-01-23 18:41:27	[redacted]	[redacted]	[redacted]	[UserAgent]
4	2021-01-23 18:41:26	[redacted]	[redacted]	[redacted]	[UserAgent]
3	2021-01-23 12:02:04	[redacted]	[redacted]	[redacted]	[UserAgent]
2	2021-01-23 12:02:04	[redacted]	[redacted]	[redacted]	[UserAgent]
1	2021-01-23 12:02:03	[redacted]	[redacted]	[redacted]	[UserAgent]

Supplemental Information

Forum Thread & Accessibility Text [1]



Воскресенье в 21:43 #1

Hey guys!

Few months ago I made a Outlook mail login page clone, but never got around using it.

I coded it completely from scratch using a little bootstrap helper classes, and reached pixel perfect 1v1 copy. I even wrote custom Javascript to simulate EXACT behavior of step switching when error is presented, and Enter is pressed vs clicked.

Login: https://i.ibb.co/VpFsG3q/Screenshot-2021-02-16-Sign-in-to-your-Microsoft-account.png
Panel: https://ibb.co/kHrpP1c (Yes, I named it EvilN3m0, since I did plan to develop this further some day.

Obviously in the latest few months the design has changed, but I can readjust it. The big question is, if is anyone interested in something like this?

Cyc199_77 и smartfiniser1

Supplemental Information (Cont.)

XSS.is Forum Post:

Hey guys!

Few months ago I made a Outlook mail login page clone, but never got around to using it.

I coded it completely from scratch using a little bootstrap helper classes, and reached pixel perfect 1v1 copy. I even wrote custom Javascript to simulate EXACT behavior of step switching when error is presented, and Enter is pressed vs clicked.

Login: <redacted>
Panel: <redacted> (Yes, I named it EvilN3m0, since I did plan to develop this further some day.

Obviously in the latest few months the design has changed, but I can readjust it. The big question is, if is anyone interested in something like this?

XSS User Reply:

YES DO IT

XSS User Reply:

Agreed, definitely do it

Sources

[1] http://<redacted>.onion

By generating the report above, we can successfully inform our supervisors or leadership of a potential threat that we have found via OSINT. There are many, many TOR sources to draw from, but as mentioned previously, one should always exercise caution when visiting unknown Onion links. There is often little to verify or research in the clearnet, since these threats are often unknown and/or not deployed at the current time.

CONCLUSION

Wrap Up

You should now feel comfortable generating OSINT reports on both known and unknown threats, regardless of clearnet or TOR sources. The most important aspect of gathering OSINT is to document your findings, as well as cite your sources and take screenshots for reference if the site or post is taken offline.

If you still do not feel confident in researching and writing these reports, I urge you to utilize the same principals in this publication with non-malicious IP's or file hashes first. Getting comfortable and familiarizing yourself with the tools can go a long way before you need to apply them.

Finally, enjoy what you do, and modify your process for your organization or for your own intelligence benefit. No guide is all-encompassing, and no specific source will have all the answers. Enjoy collecting OSINT!