Jul 28 2023

NETMANAGEIT

Intelligence Report

The resurgence of the Ursnif banking trojan

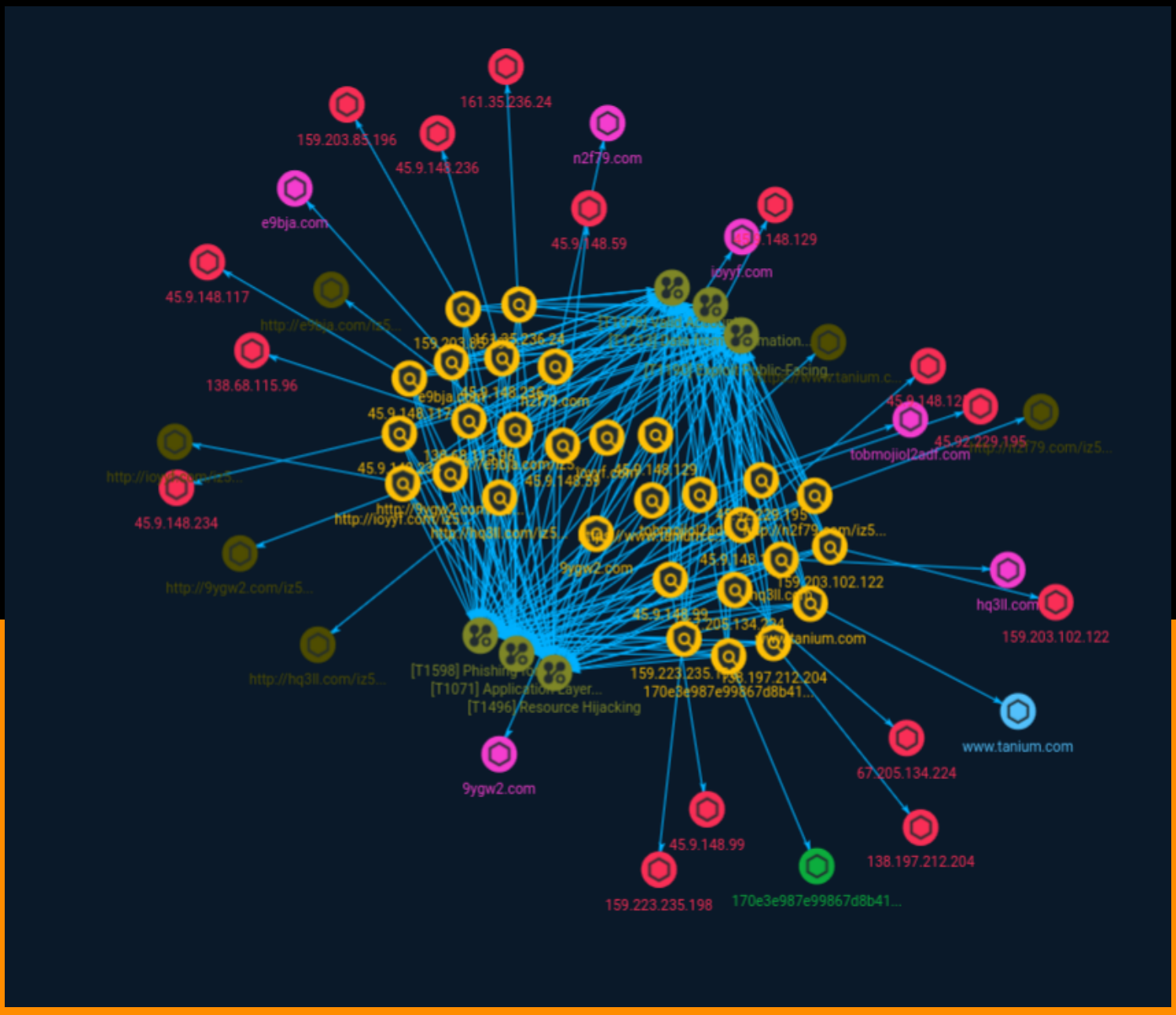

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The Ursnif banking trojan, described as May's most wanted malware, is making a resurgence across its customers' networks.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Indicator

Name
138.68.115.96
Description
CC=DE ASN=AS14061 DIGITALOCEAN-ASN
Pattern Type
stix
Pattern
[ipv4-addr:value = '138.68.115.96']
Name
http://e9bja.com/iz5/yaca.php?l=kpt4.cabFile
Pattern Type
stix
Pattern
[url:value = 'http://e9bja.com/iz5/yaca.php?l=kpt4.cabFile']

Name

http://9ygw2.com/iz5/yaca.php?l=kpt1.cabFile

Pattern Type

stix

Pattern

[url:value = 'http://9ygw2.com/iz5/yaca.php?l=kpt1.cabFile']

Name

67.205.134.224

Description

ISP: DigitalOcean, LLC **OS:** Linux ---------- Hostnames: - erp.advtechsys.net ---------- Domains: - advtechsys.net ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCqOyBNow+NBXmU2Fbeqm5loDHIvxphpG0oDOTEfID6g4kv KtEWAuF7vSeF7OC9yTJjWpvz5sxRseTgstxauxa3vrhThxISkgOq69zicqhDLaq/CkmQq/JCZl7w MbgzVtfS/O8ITC2eYrBlKsp57zkYEojJceVogWXuLI9GIU+xGcABfVCAC6Zihqv/pysRqjfsCBuX XqyzTOCKp5p218OCar61vJg5Xw2h/PjyLmeljTTxjFhlAblduXhnalW+jAArlqFzYHWxopVrdq5V J0LC+ew57SQFWn/UAzax8VYD+K+t8AtVsBZCEs7yJwlL8gYjEzyL5Vhlv6qbQ6LskPczfEJKsh4y YgTXB8uAo9OL/fRfVzLSDm14wcbM6irJOc/o4duM7abWsW0TJht7fQ0DtlNUCNgUV0c3Q+aa6csV +y+iFhxvg0BWapZtljEn16NzuiGNyQ7SZkmzARfS2x2A8Uhu+Ty5oYGQGlotkdLTmRhd/v6W3SOi iZ5G9QBndkM= Fingerprint: 64:a9:fc:ad:5c:d2:19:e7:1c:92:56:50:7a:a0:9e:9d Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com

umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Wed, 18 Jan 2023 07:40:11 GMT Content-Type: text/html Content-Length: 612 Last-Modified: Wed, 02 Feb 2022 22:25:23 GMT Connection: keep-alive ETag: "61fb04d3-264" Accept-Ranges: bytes ``` ---------- **443:** ``` HTTP/1.1 404 NOT FOUND Server: nginx/1.18.0 (Ubuntu) Date: Thu, 26 Jan 2023 19:29:15 GMT Content-Type: text/html Content-Length: 141 Connection: keep-alive ``` HEARTBLEED: 2023/01/26 19:29:24 67.205.134.224:443 - SAFE ---------- **9000:** ``` HTTP/1.1 404 Not Found Content-Security-Policy: default-src 'none' X-Content-Type-Options: nosniff Content-Type: text/html; charset=utf-8 Content-Length: 139 Date: Wed, 18 Jan 2023 23:15:01 GMT Connection: keep-alive Keep-Alive: timeout=5 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '67.205.134.224']

Name

9ygw2.com

Pattern Type

stix

Pattern

[domain-name:value = '9ygw2.com']

Name

e9bja.com

Pattern Type

stix

Pattern

[domain-name:value = 'e9bja.com']

Name

45.9.148.59

Description

CoinMiner CC=NL ASN=AS49447 Nice IT Services Group Inc.

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.9.148.59']

Name

45.9.148.117

Description

CoinMiner CC=NL ASN=AS49447 Nice IT Services Group Inc.

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.9.148.117']

Name

tobmojiol2adf.com

Pattern Type

stix

Pattern

[domain-name:value = 'tobmojiol2adf.com']

Name

170e3e987e99867d8b4115b4a2d9dea074acb56383744d469a28c5611adeba22

Description

Trojan:Linux/CoinMiner.D!MTB SHA256 of 73e5dbafa25946ed636e68d1733281e63332441d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '170e3e987e99867d8b4115b4a2d9dea074acb56383744d469a28c5611adeba22']

Name

n2f79.com

Pattern Type

stix

Pattern

[domain-name:value = 'n2f79.com']

Name

138.197.212.204

Description

ISP: DigitalOcean, LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQC2+XZEFPAzriZI6plspGyinSeqZqoXaefFKE0lueHdHDMEOXiherQyTgcHZt3zP8Tz2xLfbjp1xyIR5oCEdvpirwYvNbu/Lg31NEeKpte18pHaOUAkPQQyRRqkkbVgPFCQ6xRskpln9SeKjn29bhuF+ECF4ZK2mDFG5xvPpXvudJ8NIPj43z8IGFzy++jR+c9NKaRRCuV+WlYn/DiTZHocTYPkKMxyKne/wHlfjh8L4R+rFv3Fv9pJnr6XyxMKp8VW4D1dL1iz+2UnlooqHFl1I4A/IEHZWYJPS36zwjH32tDDdjMBBcZCR+C/zIcUz8aHVhVCZsTzu6pQ05Vrep4T Fingerprint: f1:f5:2f:3c:60:7e:81:82:d4:0f:a8:e8:63:50:c1:de Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Mon, 24 Jul 2023 05:49:12 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Sun, 24 Nov 2019 21:43:30 GMT ETag: "2aa6-5981e89beadf0" Accept-Ranges: bytes Content-Length: 10918 Vary: Accept-Encoding Content-Type: text/html ``` ---------- **443:** ``` HTTP/1.1 200 OK Date: Mon, 24 Jul 2023 07:44:38 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Sun, 24 Nov 2019 21:43:30 GMT ETag: "2aa6-5981e89beadf0" Accept-Ranges: bytes Content-Length: 10918 Vary: Accept-Encoding Content-Type: text/html
Ubuntu Logo Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it m ```

Pattern Type

stix

Pattern

[ipv4-addr:value = '138.197.212.204']

Name

http://hq3ll.com/iz5/yaca.php?l=kpt12.cabFile

Pattern Type

stix

Pattern

[url:value = 'http://hq3ll.com/iz5/yaca.php?l=kpt12.cabFile']

Name

45.9.148.129

Description

CoinMiner CC=NL ASN=AS49447 Nice IT Services Group Inc.

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.9.148.129']

Name

45.9.148.99

Description

CC=NL ASN=AS49447 Nice IT Services Group Inc.

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.9.148.99']

Name

45.9.148.236

Description

CC=NL ASN=AS49447 Nice IT Services Group Inc.

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.9.148.236']

Name

45.9.148.125

Description

CoinMiner CC=NL ASN=AS49447 Nice IT Services Group Inc.

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.9.148.125']

Name

45.9.148.234

Description

CC=NL ASN=AS49447 Nice IT Services Group Inc.

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.9.148.234']

Name

http://n2f79.com/iz5/yaca.php?l=kpt1.cabFile

Pattern Type

stix

Pattern

[url:value = 'http://n2f79.com/iz5/yaca.php?l=kpt1.cabFile']

Name

https://www.tanium.com/blog/whybusiness-email-compromise-costs-companies-more-than-ransomware-attacks/

Pattern Type

stix

Pattern

[url:value = 'https://www.tanium.com/blog/whybusiness-email-compromise-costs-companies-more-than-ransomware-attacks/']

Name

ioyyf.com

Pattern Type

stix

Pattern

[domain-name:value = 'ioyyf.com']

Name

www.tanium.com

Pattern Type

stix

Pattern

[hostname:value = 'www.tanium.com']

Name

http://ioyyf.com/iz5/yaca.php?l=kpt4.cabFile

Pattern Type

stix

Pattern

[url:value = 'http://ioyyf.com/iz5/yaca.php?l=kpt4.cabFile']

Name

45.92.229.195

Description

CC=NL ASN=AS213277 Almouroltec Servicos De Informatica E Internet Lda

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.92.229.195']

Name

hq3ll.com

Pattern Type

stix

Pattern

[domain-name:value = 'hq3ll.com']

Name

159.203.85.196

Description

Agressive IP known malicious on AbuseIPDB - countryCode: US - abuseConfidenceScore: 100 - lastReportedAt: 2023-07-28T09:15:43+00:00

Pattern Type

stix

Pattern

[ipv4-addr:value = '159.203.85.196']

Name

159.203.102.122

Description

Agressive IP known malicious on AbuseIPDB - countryCode: US - abuseConfidenceScore: 100 - lastReportedAt: 2023-07-28T08:55:35+00:00

Pattern Type

stix

Pattern

[ipv4-addr:value = '159.203.102.122']

Name

159.223.235.198

Description

ISP: DigitalOcean, LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCyPUNXDSAuLpjffIkwV+idoYfzQ/ldRYfJj1h3HAA2GCjB vBhdGJsudnk05pMOT4J+1oDlR6z3gF4aYKuP0KSir17nfJZEjxvVXqyEpJjsF44IXdiN2St1U2d6 Yp6jbb0aERd+TsT7Ct9JIf9u1I1a0IcyENZu+LvWOqeKwjIBRRwt+2vKEUgtgMyXXW/Zkrx2ROJE 8aMYRl2LACpnvN3KNiYEWN0eEwtkFk2Mag5j9/5k1/ Oy+e6dmR0EofAWoiaumm+5r89OsKBHPDJs QAyhCZiTOLqq0qKbcSwkSRVOyiBy9TAC+5VL3KjoOpvP685el49s6buTWkjw+yBWgx+Leedq4WPD 1GAfYZ9MDcHG7v4IPG0juWMIrd56udAgvdiDHLrdFHP56rMC4gBZZz3NnBKPl7SQHAEDRTqccbM m dzADhaybvzwoH6piFeLczFLAzKfchXojtZOWSOI+hwQskPErIoUwK4/5da11nXMgzM9iykNBKMQE y6CZkDaTPiU= Fingerprint: 26:62:44:26:24:80:b9:9f:61:9c:fe:4f:87:bc:18:41 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms:

chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Sun, 01 Jan 2023 15:51:55 GMT Server: Apache/2.4.41 (Ubuntu) Last-Modified: Mon, 30 May 2022 07:13:49 GMT ETag: "2aa6-5e03565d67dc3" Accept-Ranges: bytes Content-Length: 10918 Vary: Accept-Encoding Content-Type: text/html ``` ---------- **8545:** ``` HTTP/1.1 200 OK Vary: Origin Date: Sun, 15 Jan 2023 00:29:45 GMT Content-Length: 0 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '159.223.235.198']

Name

161.35.236.24

Description

ISP: DigitalOcean, LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Thu, 26 Jan 2023 06:11:04 GMT Content-Type: text/html Content-Length: 0 Last-Modified: Wed, 02 Nov 2022 19:25:28 GMT Connection: keep-alive ETag: "6362c428-0" Accept-Ranges: bytes ``` ---------- **5432:** ``` PostgreSQL fe_sendauth: no password supplied ``` ----------

Pattern Type

stix

Pattern

```
[ipv4-addr:value = '161.35.236.24']
```

Attack-Pattern

Name

Phishing for Information

ID

T1598

Description

Adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Phishing for information is different from [Phishing](https://attack.mitre.org/techniques/T1566) in that the objective is gathering data from the victim rather than executing malicious code. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass credential harvesting campaigns. Adversaries may also try to obtain information directly through the exchange of emails, instant messages, or other electronic conversation means.(Citation: ThreatPost Social Media Phishing)(Citation: TrendMictro Phishing)(Citation: PCMag FakeLogin)(Citation: Sophos Attachment)(Citation: GitHub Phishery) Victims may also receive phishing messages that direct them to call a phone number where the adversary attempts to collect confidential information.(Citation: Avertium callback phishing) Phishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)) and/or sending multiple, seemingly urgent messages. Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce)

Phishing for information may also involve evasive techniques, such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)). (Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014)

Name

Data from Information Repositories

ID

T1213

Description

Adversaries may leverage information repositories to mine valuable information. Information repositories are tools that allow for storage of information, typically to facilitate collaboration or information sharing between users, and can store a wide variety of data that may aid adversaries in further objectives, or direct access to the target information. Adversaries may also abuse external sharing features to share sensitive documents with recipients outside of the organization. The following is a brief list of example information that may hold potential value to an adversary and may also be found on an information repository: * Policies, procedures, and standards * Physical / logical network diagrams * System architecture diagrams * Technical system documentation * Testing / development credentials * Work / project schedules * Source code snippets * Links to network shares and other internal resources Information stored in a repository may vary based on the specific instance or environment. Specific common information repositories include web-based platforms such as [Sharepoint](https://attack.mitre.org/techniques/T1213/002) and [Confluence](https://attack.mitre.org/techniques/T1213/001), specific services such as Code Repositories, IaaS databases, enterprise databases, and other storage infrastructure such as SQL Server.

Name

Resource Hijacking

ID

T1496

Description

Adversaries may leverage the resources of co-opted systems in order to solve resource intensive problems, which may impact system and/or hosted service availability. One common purpose for Resource Hijacking is to validate transactions of cryptocurrency networks and earn virtual currency. Adversaries may consume enough system resources to negatively impact and/or cause affected machines to become unresponsive.(Citation: Kaspersky Lazarus Under The Hood Blog 2017) Servers and cloud-based systems are common targets because of the high potential for available resources, but user endpoint systems may also be compromised and used for Resource Hijacking and cryptocurrency mining.(Citation: CloudSploit - Unused AWS Regions) Containerized environments may also be targeted due to the ease of deployment via exposed APIs and the potential for scaling mining activities by deploying or compromising multiple containers within an environment or cluster.(Citation: Unit 42 Hildegard Malware)(Citation: Trend Micro Exposed Docker APIs) Additionally, some cryptocurrency mining malware identify then kill off processes for competing malware to ensure it’s not competing for resources.(Citation: Trend Micro War of Crypto Miners) Adversaries may also use malware that leverages a system's network bandwidth as part of a botnet in order to facilitate [Network Denial of Service](https://attack.mitre.org/techniques/T1498) campaigns and/or to seed malicious torrents.(Citation: GoBotKR)

Name

Valid Accounts

ID

T1078

Description

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop.(Citation: volexity_0day_sophos_FW) Compromised credentials may also

grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence. In some cases, adversaries may abuse inactive accounts: for example, those belonging to individuals who are no longer part of an organization. Using these accounts may allow the adversary to evade detection, as the original account user will not be present to identify any anomalous activity taking place on their account.(Citation: CISA MFA PrintNightmare) The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.(Citation: TechNet Credential Theft)

Name

Exploit Public-Facing Application

ID

T1190

Description

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases,

the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities. (Citation: OWASP Top 10)(Citation: CWE top 25)

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Domain-Name

Value
n2f79.com
ioyyf.com
e9bja.com
tobmojiol2adf.com
9ygw2.com
hq3ll.com

StixFile

Value
170e3e987e99867d8b4115b4a2d9dea074acb56383744d469a28c5611adeba22

Hostname

Value
www.tanium.com

IPv4-Addr

Value
45.9.148.117
45.9.148.125
67.205.134.224
45.9.148.236
138.197.212.204
45.9.148.234
45.9.148.59
45.92.229.195
138.68.115.96
45.9.148.129
45.9.148.99
159.203.85.196
159.223.235.198

161.35.236.24

159.203.102.122

Url

Value
http://ioyyf.com/iz5/yaca.php?l=kpt4.cabFile
http://n2f79.com/iz5/yaca.php?l=kpt1.cabFile
http://9ygw2.com/iz5/yaca.php?l=kpt1.cabFile
https://www.tanium.com/blog/whybusiness-email-compromise-costs-companies-more-than-ransomware-attacks/
http://hq3ll.com/iz5/yaca.php?l=kpt12.cabFile
http://e9bja.com/iz5/yaca.php?l=kpt4.cabFile

External References

- https://otx.alienvault.com/pulse/64c3b9dc8c9f288d10c98fe9
- https://darktrace.com/blog/the-resurgence-of-the-ursnif-banking-trojan