Sep 21 2023

NETMANAGEIT

Intelligence Report

#StopRansomware: Snatch Ransomware

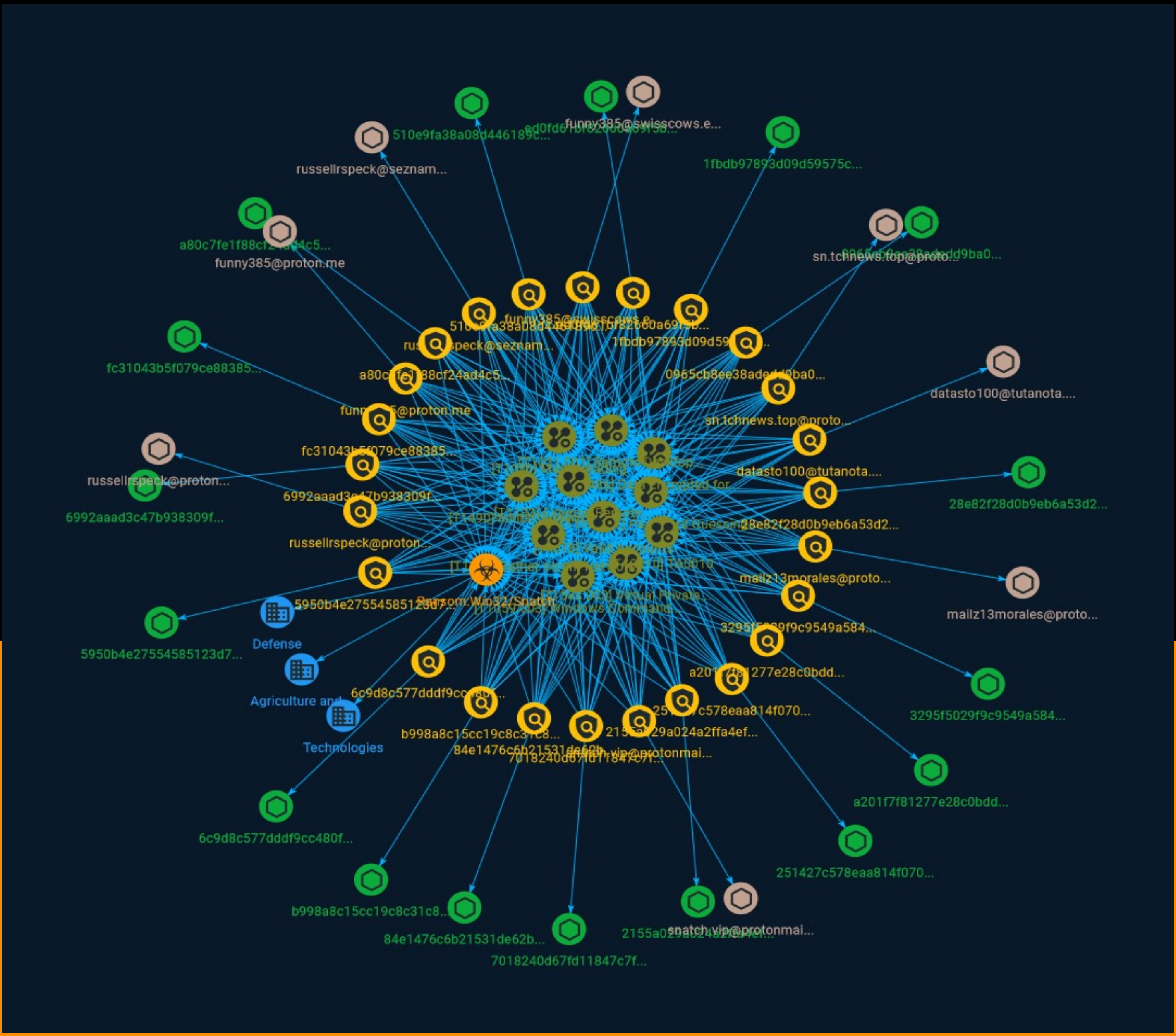

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Since mid-2021, Snatch threat actors have consistently evolved their tactics to take advantage of current trends in the cybercriminal space and leveraged the successes of other ransomware variants' operations. Snatch threat actors conduct ransomware operations involving data exfiltration and double extortion. After data exfiltration often involves direct communications with victims demanding ransom, Snatch threat actors may threaten victims with double extortion, where the victims' data will be posted on Snatch's extortion blog if the ransom goes unpaid.

Confidence

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

15 / 100

Attack-Pattern

Name

Password Guessing

ID

T1110.001

Description

Adversaries with no prior knowledge of legitimate credentials within the system or environment may guess passwords to attempt access to accounts. Without knowledge of the password for an account, an adversary may opt to systematically guess the password using a repetitive or iterative mechanism. An adversary may guess login credentials without prior knowledge of system or environment passwords during an operation by using a list of common passwords. Password guessing may or may not take into account the target's policies on password complexity or use policies that may lock accounts out after a number of failed attempts. Guessing passwords can be a risky option because it could cause numerous authentication failures and account lockouts, depending on the organization's login failure policies. (Citation: Cylance Cleaver) Typically, management services over commonly used ports are used when guessing passwords. Commonly targeted services include the following: * SSH (22/TCP) * Telnet (23/TCP) * FTP (21/TCP) * NetBIOS / SMB / Samba (139/TCP & 445/TCP) * LDAP (389/TCP) * Kerberos (88/TCP) * RDP / Terminal Services (3389/TCP) * HTTP/HTTP Management Services (80/TCP & 443/TCP) * MSSQL (1433/TCP) * Oracle (1521/TCP) * MySQL (3306/TCP) * VNC (5900/TCP) * SNMP (161/UDP and 162/TCP/UDP) In addition to management services, adversaries may "target single sign-on (SSO) and cloud-based applications utilizing federated authentication protocols," as well as externally facing email applications, such as Office 365.(Citation: US-CERT TA18-068A 2018). Further, adversaries may abuse network device interfaces (such as `wlanAPI`) to brute force accessible wifi-router(s) via wireless authentication protocols. (Citation: Trend Micro Emotet 2020) In default environments, LDAP and Kerberos connection attempts are less likely to trigger events over SMB, which creates Windows "logon failure" event ID 4625.

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
Masquerading

ID
T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)

Name

Virtual Private Server

ID

T1583.003

Description

Adversaries may rent Virtual Private Servers (VPSs) that can be used during targeting. There exist a variety of cloud service providers that will sell virtual machines/containers as a service. By utilizing a VPS, adversaries can make it difficult to physically tie back operations to them. The use of cloud infrastructure can also make it easier for adversaries to rapidly provision, modify, and shut down their infrastructure. Acquiring a VPS for use in later stages of the adversary lifecycle, such as Command and Control, can allow adversaries to benefit from the ubiquity and trust associated with higher reputation cloud service providers. Adversaries may also acquire infrastructure from VPS service providers that are known for renting VPSs with minimal registration information, allowing for more anonymous acquisitions of infrastructure.(Citation: TrendmicroHideoutsLease)

Name

Inhibit System Recovery

ID

T1490

Description

Adversaries may delete or remove built-in data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery.(Citation: Talos Olympic Destroyer 2018)(Citation: FireEye WannaCry 2017) This may deny access to available backups and recovery options. Operating systems may contain features that can help fix corrupted systems, such as a backup catalog, volume shadow copies, and automatic repair features. Adversaries may disable or delete system recovery features to augment the effects of [Data Destruction](https://attack.mitre.org/techniques/T1485) and [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486).(Citation: Talos Olympic Destroyer 2018)(Citation: FireEye WannaCry 2017) Furthermore, adversaries may disable recovery notifications, then corrupt backups.(Citation: disable_notif_synology_ransom) A number of native Windows utilities have been used by adversaries to disable or delete system recovery features: * `vssadmin.exe` can be used to delete all volume shadow copies on a system - `vssadmin.exe delete shadows /all /quiet` * [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) can be used to delete volume shadow copies - `wmic shadowcopy delete` * `wbadmin.exe` can be used to delete the Windows Backup Catalog - `wbadmin.exe delete catalog -quiet` * `bcdedit.exe` can be used to disable automatic Windows recovery features by modifying boot configuration data - `bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no` * `REAgentC.exe` can be used to disable Windows Recovery Environment (WinRE) repair/recovery options of an infected system On network devices, adversaries may leverage [Disk Wipe](https://attack.mitre.org/techniques/T1561) to delete backup firmware images and reformat the file system, then [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529) to reload the device. Together this activity may leave network devices completely inoperable and inhibit recovery operations. Adversaries may also delete “online” backups that are connected to their network – whether via network storage media or through folders that sync to cloud services.(Citation: ZDNet Ransomware Backups 2020) In cloud environments, adversaries may disable versioning and backup policies and delete snapshots, machine images, and prior versions of objects designed to be used in disaster recovery scenarios.(Citation: Dark Reading Code Spaces Cyber Attack)(Citation: Rhino Security Labs AWS S3 Ransomware)

Name

Data Encrypted for Impact

ID

T1486

Description

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.(Citation: US-CERT Ransomware 2016)(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017)(Citation: US-CERT SamSam 2018) In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529), in order to unlock and/or gain access to manipulate these files.(Citation: CarbonBlack Conti July 2020) In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.(Citation: US-CERT NotPetya 2017) To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017) Encryption malware may also leverage [Internal Defacement](https://attack.mitre.org/techniques/T1491/001), such as changing victim wallpapers, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").(Citation: NHS Digital Egregor Nov 2020) In cloud environments, storage objects within compromised accounts may also be encrypted.(Citation: Rhino S3 Ransomware Part 1)

Name

Windows Command Shell

ID

T1059.003

Description
Adversaries may abuse the Windows command shell for execution. The Windows command shell ([cmd](https://attack.mitre.org/software/S0106)) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands. The command prompt can be invoked remotely via [Remote Services](https://attack.mitre.org/techniques/T1021) such as [SSH](https://attack.mitre.org/techniques/T1021/004).(Citation: SSH in Windows) Batch files (ex: .bat or .cmd) also provide the shell with a list of sequential commands to run, as well as normal scripting operations such as conditionals and loops. Common uses of batch files include long or repetitive tasks, or the need to run the same set of commands on multiple systems. Adversaries may leverage [cmd](https://attack.mitre.org/software/S0106) to execute various commands and payloads. Common uses include [cmd](https://attack.mitre.org/software/S0106) to execute a single command, or abusing [cmd](https://attack.mitre.org/software/S0106) interactively with input and output forwarded over a command and control channel.

Name
External Remote Services

ID
T1133

Description
Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006) and [VNC](https://attack.mitre.org/techniques/T1021/005) can also be used externally.(Citation: MacOS VNC software for Remote Desktop) Access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation. Access may also be gained through an exposed service that doesn’t require authentication. In

containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

Name

TA0010

ID

TA0010

Name

Gather Victim Network Information

ID

T1590

Description

Adversaries may gather information about the victim's networks that can be used during targeting. Information about networks may include a variety of details, including administrative data (ex: IP ranges, domain names, etc.) as well as specifics regarding its topology and operations. Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about networks may also be exposed to adversaries via online or other accessible data sets (ex: [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)).(Citation: WHOIS)(Citation: DNS Dumpster)(Citation: Circl Passive DNS) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [Trusted Relationship](https://attack.mitre.org/techniques/T1199)).

Name

Remote Desktop Protocol

ID

T1021.001

Description

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a computer using the Remote Desktop Protocol (RDP). The adversary may then perform actions as the logged-on user. Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS).(Citation: TechNet Remote Desktop Services) Adversaries may connect to a remote system over RDP/RDS to expand access if the service is enabled and allows access to accounts with known credentials. Adversaries will likely use Credential Access techniques to acquire credentials to use with RDP. Adversaries may also use RDP in conjunction with the [Accessibility Features](https://attack.mitre.org/techniques/T1546/008) or [Terminal Services DLL](https://attack.mitre.org/techniques/T1505/005) for Persistence.(Citation: Alperovitch Malware)

Sector

Name
Agriculture and agribusiness
Description
Private entities specialized in the growth, culture, transport and transformation of plants or livestock for food.
Name
Defense
Description
Public and private entities involved in the conception and production of weapons and the planning and conducting of military operations.
Name
Technologies
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

Indicator

Name

russellrspeck@seznam.cz

Pattern Type

stix

Pattern

[email-addr:value = 'russellrspeck@seznam.cz']

Name

3295f5029f9c9549a584fa13bc6c25520b4ff9a4b2feb1d9e935cc9e4e0f0924

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3295f5029f9c9549a584fa13bc6c25520b4ff9a4b2feb1d9e935cc9e4e0f0924']

Name

5950b4e27554585123d7fca44e83169375c6001201e3bf26e57d079437e70bcd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'5950b4e27554585123d7fca44e83169375c6001201e3bf26e57d079437e70bcd']

Name

1fbdb97893d09d59575c3ef95df3c929fe6b6ddf1b273283e4efadf94cdc802d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'1fbdb97893d09d59575c3ef95df3c929fe6b6ddf1b273283e4efadf94cdc802d']

Name

snatch.vip@protonmail.com

Pattern Type

stix

Pattern

[email-addr:value = 'snatch.vip@protonmail.com']

Name
funny385@proton.me
Pattern Type
stix
Pattern
[email-addr:value = 'funny385@proton.me']
Name
28e82f28d0b9eb6a53d22983e21a9505ada925ebb61382fabebd76b8c4acff7c
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '28e82f28d0b9eb6a53d22983e21a9505ada925ebb61382fabebd76b8c4acff7c']
Name
b998a8c15cc19c8c31c89b30f692a40b14d7a6c09233eb976c07f19a84eccb40
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' =
'b998a8c15cc19c8c31c89b30f692a40b14d7a6c09233eb976c07f19a84eccb40']

Name

funny385@swisscows.email

Pattern Type

stix

Pattern

[email-addr:value = 'funny385@swisscows.email']

Name

251427c578eaa814f07037fbe6e388b3bc86ed3800d7887c9d24e7b94176e30d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'251427c578eaa814f07037fbe6e388b3bc86ed3800d7887c9d24e7b94176e30d']

Name

6992aaad3c47b938309fc1e6f37179eb51f028536f8afc02e4986312e29220c0

Pattern Type

stix

Pattern
[file:hashes.'SHA-256' = '6992aaad3c47b938309fc1e6f37179eb51f028536f8afc02e4986312e29220c0']
Name
sn.tchnews.top@protonmail.me
Pattern Type
stix
Pattern
[email-addr:value = 'sn.tchnews.top@protonmail.me']
Name
7018240d67fd11847c7f9737eaaae45794b37a5c27ffd02beaacaf6ae13352b3
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '7018240d67fd11847c7f9737eaaae45794b37a5c27ffd02beaacaf6ae13352b3']
Name
a80c7fe1f88cf24ad4c55910a9f2189f1eedad25d7d0fd53dbfe6bdd68912a84
Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a80c7fe1f88cf24ad4c55910a9f2189f1eedad25d7d0fd53dbfe6bdd68912a84']

Name

mailz13morales@proton.me

Pattern Type

stix

Pattern

[email-addr:value = 'mailz13morales@proton.me']

Name

6c9d8c577dddf9cc480f330617e263a6ee4461651b4dec1f7215bda77df911e7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6c9d8c577dddf9cc480f330617e263a6ee4461651b4dec1f7215bda77df911e7']

Name

ed0fd61bf82660a69f5bfe0e66457cfe56d66dd2b310e9e97657c37779aef65d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'ed0fd61bf82660a69f5bfe0e66457cfe56d66dd2b310e9e97657c37779aef65d']

Name

2155a029a024a2ffa4eff9108ac15c7db527ca1c8f89ccfd94cc3a70b77cfc57

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'2155a029a024a2ffa4eff9108ac15c7db527ca1c8f89ccfd94cc3a70b77cfc57']

Name

fc31043b5f079ce88385883668eeebba76a62f77954a960fb03bf46f47dbb066

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'fc31043b5f079ce88385883668eeebba76a62f77954a960fb03bf46f47dbb066']

Name

datasto100@tutanota.com

Pattern Type

stix

Pattern

[email-addr:value = 'datasto100@tutanota.com']

Name

84e1476c6b21531de62bbac67e52ab2ac14aa7a30f504ecf33e6b62aa33d1fe5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '84e1476c6b21531de62bbac67e52ab2ac14aa7a30f504ecf33e6b62aa33d1fe5']

Name

510e9fa38a08d446189c34fe6125295f410b36f00aceb65e7b4508e9d7c4e1d1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '510e9fa38a08d446189c34fe6125295f410b36f00aceb65e7b4508e9d7c4e1d1']

Name

a201f7f81277e28c0bdd680427b979aee70e42e8a98c67f11e7c83d02f8fe7ae

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a201f7f81277e28c0bdd680427b979aee70e42e8a98c67f11e7c83d02f8fe7ae']

Name

russellrspeck@protonmail.com

Pattern Type

stix

Pattern

[email-addr:value = 'russellrspeck@protonmail.com']

Name

0965cb8ee38adedd9ba06bdad9220a35890c2df0e4c78d0559cd6da653bf740f

Pattern Type

stix

Pattern
[file:hashes.'SHA-256' = '0965cb8ee38adedd9ba06bdad9220a35890c2df0e4c78d0559cd6da653bf740f']

Malware

Name
Ransom:Win32/Snatch

Email-Addr

Value
funny385@swisscows.email
russellrspeck@protonmail.com
datasto100@tutanota.com
sn.tchnews.top@protonmail.me
funny385@proton.me
snatch.vip@protonmail.com
russellrspeck@seznam.cz
mailz13morales@proton.me

StixFile

Value
1fbdb97893d09d59575c3ef95df3c929fe6b6ddf1b273283e4efadf94cdc802d
510e9fa38a08d446189c34fe6125295f410b36f00aceb65e7b4508e9d7c4e1d1
6c9d8c577dddf9cc480f330617e263a6ee4461651b4dec1f7215bda77df911e7
2155a029a024a2ffa4eff9108ac15c7db527ca1c8f89ccfd94cc3a70b77cfc57
7018240d67fd11847c7f9737eaaae45794b37a5c27ffd02beaacaf6ae13352b3
28e82f28d0b9eb6a53d22983e21a9505ada925ebb61382fabebd76b8c4acff7c
3295f5029f9c9549a584fa13bc6c25520b4ff9a4b2feb1d9e935cc9e4e0f0924
a201f7f81277e28c0bdd680427b979aee70e42e8a98c67f11e7c83d02f8fe7ae
a80c7fe1f88cf24ad4c55910a9f2189f1eedad25d7d0fd53dbfe6bdd68912a84
84e1476c6b21531de62bbac67e52ab2ac14aa7a30f504ecf33e6b62aa33d1fe5
b998a8c15cc19c8c31c89b30f692a40b14d7a6c09233eb976c07f19a84eccb40
6992aaad3c47b938309fc1e6f37179eb51f028536f8afc02e4986312e29220c0
5950b4e27554585123d7fca44e83169375c6001201e3bf26e57d079437e70bcd

0965cb8ee38adedd9ba06bdad9220a35890c2df0e4c78d0559cd6da653bf740f
ed0fd61bf82660a69f5bfe0e66457cfe56d66dd2b310e9e97657c37779aef65d
251427c578eaa814f07037fbe6e388b3bc86ed3800d7887c9d24e7b94176e30d
fc31043b5f079ce88385883668eeebba76a62f77954a960fb03bf46f47dbb066

External References

- https://otx.alienvault.com/pulse/650b084397be16067e355dcf
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-263a