Sep 18 2023

NETMANAGEIT

Intelligence Report

Threat Group Assessment: Turla (aka Pensive Ursa)

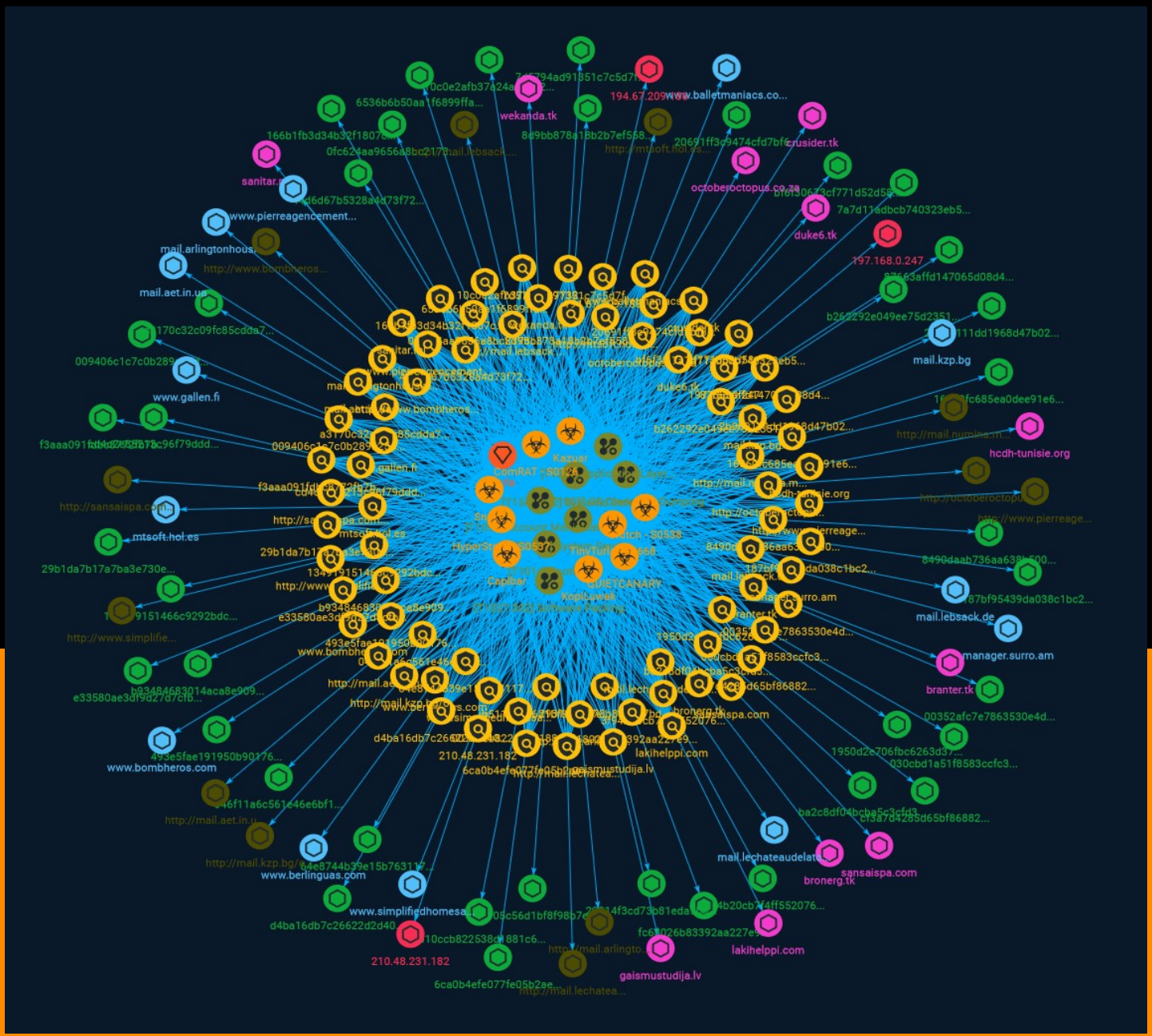

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A threat assessment of Turla (aka Pensive Ursa) breaks down this Russian-based APT's arsenal and techniques used, covering the top 10 active malware employed.

Confidence

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

15 / 100

Attack-Pattern

Name
OS Credential Dumping
ID
T1003
Description
Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.
Name
Rootkit
ID
T1014
Description
Adversaries may use rootkits to hide the presence of programs, files, network connections, services, drivers, and other system components. Rootkits are programs that hide the

existence of malware by intercepting/hooking and modifying operating system API calls that supply system information. (Citation: Symantec Windows Rootkits) Rootkits or rootkit enabling functionality may reside at the user or kernel level in the operating system or lower, to include a hypervisor, Master Boot Record, or [System Firmware](https://attack.mitre.org/techniques/T1542/001). (Citation: Wikipedia Rootkit) Rootkits have been seen for Windows, Linux, and Mac OS X systems. (Citation: CrowdStrike Linux Rootkit) (Citation: BlackHat Mac OSX Rootkit)

Name

Systemd Service

ID

T1543.002

Description

Adversaries may create or modify systemd services to repeatedly execute malicious payloads as part of persistence. Systemd is a system and service manager commonly used for managing background daemon processes (also known as services) and other system resources.(Citation: Linux man-pages: systemd January 2014) Systemd is the default initialization (init) system on many Linux distributions replacing legacy init systems, including SysVinit and Upstart, while remaining backwards compatible. Systemd utilizes unit configuration files with the `.service` file extension to encode information about a service's process. By default, system level unit files are stored in the `/systemd/system` directory of the root owned directories (`/`). User level unit files are stored in the `/systemd/user` directories of the user owned directories (`$HOME`). (Citation: lambert systemd 2022) Service unit files use the following directives to execute system commands: (Citation: freedesktop systemd.service) * `ExecStart`, `ExecStartPre`, and `ExecStartPost` directives cover execution of commands when a service is started manually by `systemctl`, or on system start if the service is set to automatically start. * `ExecReload` directive covers when a service restarts. * `ExecStop`, `ExecStopPre`, and `ExecStopPost` directives cover when a service is stopped. Adversaries may abuse systemd functionality to establish persistent access to victim systems by creating and/or modifying service unit files systemd uses upon reboot or starting a service.(Citation: Anomali Rocke March 2019) Adversaries may also place symbolic links in these directories, enabling systemd to find these payloads regardless of where they reside on the filesystem. The `.service` file's `User` directive can be used to run service as a specific user, which could result in privilege

escalation based on specific user/group permissions.(Citation: Rapid7 Service Persistence 22JUNE2016)

Name

System Service Discovery

ID

T1007

Description

Adversaries may try to gather information about registered local system services. Adversaries may obtain information about services using tools as well as OS utility commands such as `sc query`, `tasklist /svc`, `systemctl --type=service`, and `net start`. Adversaries may use the information from [System Service Discovery](https://attack.mitre.org/techniques/T1007) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Name

Account Manipulation

ID

T1098

Description

Adversaries may manipulate accounts to maintain access to victim systems. Account manipulation may consist of any action that preserves adversary access to a compromised account, such as modifying credentials or permission groups. These actions could also include account activity designed to subvert security policies, such as performing iterative password updates to bypass password duration policies and preserve the life of compromised credentials. In order to create or manipulate accounts, the adversary must already have sufficient permissions on systems or the domain. However, account

manipulation may also lead to privilege escalation where modifications grant access to additional roles, permissions, or higher-privileged [Valid Accounts](https://attack.mitre.org/techniques/T1078).

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.

Name

Software Packing

ID

T1027.002

Description

Adversaries may perform software packing or virtual machine software protection to conceal their code. Software packing is a method of compressing or encrypting an executable. Packing an executable changes the file signature in an attempt to avoid signature-based detection. Most decompression techniques decompress the executable code in memory. Virtual machine software protection translates an executable's original code into a special format that only a special virtual machine can run. A virtual machine is

then called to run this code.(Citation: ESET FinFisher Jan 2018) Utilities used to perform software packing are called packers. Example packers are MPRESS and UPX. A more comprehensive list of known packers is available, but adversaries may create their own packing techniques that do not leave the same artifacts as well-known packers to evade defenses.(Citation: Awesome Executable Packing)

Indicator

Name
a3170c32c09fc85cdda778a5c20a3dab144b6d1dd9996ba8340866e0081c7642
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'a3170c32c09fc85cdda778a5c20a3dab144b6d1dd9996ba8340866e0081c7642']
Name
b262292e049ee75d235164df98fa8ed09a9e2a30c5432623856bafd4bd44d801
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'b262292e049ee75d235164df98fa8ed09a9e2a30c5432623856bafd4bd44d801']
Name

046f11a6c561e46e6bf199ab7f50e74a4d2aaead68cdbd6ce44b37b5b4964758

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '046f11a6c561e46e6bf199ab7f50e74a4d2aaead68cdbd6ce44b37b5b4964758']

Name

http://mail.lebsack.de/MICROSOFT.EXCHANGE.MAILBOXREPLICATIONSERVICE.PROXYSERVICE/RPCWITCHERT/SYNC

Pattern Type

stix

Pattern

[url:value = 'http://mail.lebsack.de/MICROSOFT.EXCHANGE.MAILBOXREPLICATIONSERVICE.PROXYSERVICE/RPCWITCHERT/SYNC']

Name

1950d2e706fbc6263d376c0c4f16bd5acfd543248ee072657ba3dd62da8427eb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1950d2e706fbc6263d376c0c4f16bd5acfd543248ee072657ba3dd62da8427eb']

Name

b93484683014aca8e909c9b5648d8f0ac21a45d0c193f6ca40f0b01d2464c1c4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b93484683014aca8e909c9b5648d8f0ac21a45d0c193f6ca40f0b01d2464c1c4']

Name

http://mtsoft.hol.es/wp-content/gallery/

Pattern Type

stix

Pattern

[url:value = 'http://mtsoft.hol.es/wp-content/gallery/']

Name

b51105c56d1bf8f98b7e924aa5caded8322d037745a128781fa0bc23841d1e70

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b51105c56d1bf8f98b7e924aa5caded8322d037745a128781fa0bc23841d1e70']

Name

44d6d67b5328a4d73f72d8a0f9d39fe4bb6539609f90f169483936a8b3b88316

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '44d6d67b5328a4d73f72d8a0f9d39fe4bb6539609f90f169483936a8b3b88316']

Name

http://mail.numina.md/owa/scripts/logon.aspx

Pattern Type

stix

Pattern

[url:value = 'http://mail.numina.md/owa/scripts/logon.aspx']

Name

www.berlinguas.com

Pattern Type

stix

Pattern

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

Name

octoberoctopus.co.za

Pattern Type

stix

Pattern

[domain-name:value = 'octoberoctopus.co.za']

Name

29314f3cd73b81eda7bd90c66f659235e6bb900e499c9cc7057d10a9083a0b94

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '29314f3cd73b81eda7bd90c66f659235e6bb900e499c9cc7057d10a9083a0b94']

Name

www.gallen.fi

Pattern Type
stix
Pattern
[hostname:value = 'www.gallen.fi']
Name
197.168.0.247
Pattern Type
stix
Pattern
[ipv4-addr:value = '197.168.0.247']
Name
64e8744b39e15b76311733014327311acd77330f8a135132f020eac78199ac8a
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '64e8744b39e15b76311733014327311acd77330f8a135132f020eac78199ac8a']
Name

0fc624aa9656a8bc21731bfc47fd7780da38a7e8ad7baf1529ccd70a5bb07852

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0fc624aa9656a8bc21731bfc47fd7780da38a7e8ad7baf1529ccd70a5bb07852']

Name

8490daab736aa638b500b27c962a8250bbb8615ae1c68ef77494875ac9d2ada2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8490daab736aa638b500b27c962a8250bbb8615ae1c68ef77494875ac9d2ada2']

Name

493e5fae191950b901764868b065ddddffa4f4c9b497022ee2f998b4a94f0fc2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '493e5fae191950b901764868b065ddddffa4f4c9b497022ee2f998b4a94f0fc2']

Name

bf6f30673cf771d52d589865675a293dc5c3668a956d0c2fc0d9403424d429b2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bf6f30673cf771d52d589865675a293dc5c3668a956d0c2fc0d9403424d429b2']

Name

mail.lechateaudelatour.fr

Pattern Type

stix

Pattern

[hostname:value = 'mail.lechateaudelatour.fr']

Name

http://www.bombheros.com/wp-content/languages/index.php

Pattern Type

stix

Pattern

[url:value = 'http://www.bombheros.com/wp-content/languages/index.php']

Name

http://www.pierreagencement.fr/wp-content/languages/index.php

Pattern Type

stix

Pattern

[url:value = 'http://www.pierreagencement.fr/wp-content/languages/index.php']

Name

www.simplifiedhomesales.com

Pattern Type

stix

Pattern

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

Name

8d9bb878a18b2b7ef558504e78a59eb644f83a63679658533ff8accf0b85fda3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8d9bb878a18b2b7ef558504e78a59eb644f83a63679658533ff8accf0b85fda3']

Name

ba2c8df04bcba5c3cfd343a59d8b59b76779e6c27eb27b7ac73ded97e08f0f39

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ba2c8df04bcba5c3cfd343a59d8b59b76779e6c27eb27b7ac73ded97e08f0f39']

Name

134919151466c9292bdcb7c24c32c841a5183d880072b0ad5e8b3a3a830afef8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '134919151466c9292bdcb7c24c32c841a5183d880072b0ad5e8b3a3a830afef8']

Name

duke6.tk

Pattern Type

stix

Pattern

[domain-name:value = 'duke6.tk']

Name

http://mail.arlingtonhousing.us/outlook/api/logoff.aspx

Pattern Type

stix

Pattern

[url:value = 'http://mail.arlingtonhousing.us/outlook/api/logoff.aspx']

Name

www.pierreagencement.fr

Pattern Type

stix

Pattern

[hostname:value = 'www.pierreagencement.fr']

Name

mail.lebsack.de

Pattern Type

stix

Pattern

[hostname:value = 'mail.lebsack.de']

Name

www.bombheros.com

Pattern Type

stix

Pattern

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

Name

20691ff3c9474cfd7bf6fa3f8720eb7326e6f87f64a1f190861589c1e7397fa5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '20691ff3c9474cfd7bf6fa3f8720eb7326e6f87f64a1f190861589c1e7397fa5']

Name

3f94b20cb7f4ff55207660649ebbb02679c991fe03efbcb0bd3840fc7f0bd527

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3f94b20cb7f4ff55207660649ebbb02679c991fe03efbcb0bd3840fc7f0bd527']

Name

cd4c2e85213c96f79ddda564242efec3b970eded8c59f1f6f4d9a420eb8f1858

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cd4c2e85213c96f79ddda564242efec3b970eded8c59f1f6f4d9a420eb8f1858']

Name

mail.kzp.bg

Pattern Type

stix

Pattern

[hostname:value = 'mail.kzp.bg']

Name

0010ccb822538d1881c61be874af49382c44b6c9cb665081cf0f672cbed5b6a5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0010ccb822538d1881c61be874af49382c44b6c9cb665081cf0f672cbed5b6a5']

Name

6536b6b50aa1f6899ffa90aaf4b1b67c0ae0f6c0441016f5308b37c12141c61d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6536b6b50aa1f6899ffa90aaf4b1b67c0ae0f6c0441016f5308b37c12141c61d']

Name

branter.tk

Pattern Type

stix

Pattern

[domain-name:value = 'branter.tk']

Name

http://www.simplifiedhomesales.com/wp-includes/images/index.php

Pattern Type

stix

Pattern

[url:value = 'http://www.simplifiedhomesales.com/wp-includes/images/index.php']

Name

87663affd147065d08d4fe76d9a18b0d7d85fab68cf9f5ac96cfdfff3f27ffd2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '87663affd147065d08d4fe76d9a18b0d7d85fab68cf9f5ac96cfdfff3f27ffd2']

Name

lakihelppi.com

Pattern Type

stix

Pattern

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

Name

mail.arlingtonhousing.us

Pattern Type

stix

Pattern

[hostname:value = 'mail.arlingtonhousing.us']

Name

187bf95439da038c1bc291619507ff5e426d250709fa5e3eda7fda99e1c9854c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '187bf95439da038c1bc291619507ff5e426d250709fa5e3eda7fda99e1c9854c']

Name

http://mail.aet.in.ua/outlook/api/logoff.aspx

Pattern Type

stix

Pattern

[url:value = 'http://mail.aet.in.ua/outlook/api/logoff.aspx']

Name

7d5794ad91351c7c5d7fbad8e83e3b71a09baac65fb09ca75d8d18339d24a46f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7d5794ad91351c7c5d7fbad8e83e3b71a09baac65fb09ca75d8d18339d24a46f']

Name

sansaispa.com

Pattern Type

stix

Pattern

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

Name

mtsoft.hol.es

Pattern Type

stix

Pattern

[hostname:value = 'mtsoft.hol.es']

Name

16860fc685ea0dee91e65e253062153ac6c886fdd73a3020c266601f58038a61

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '16860fc685ea0dee91e65e253062153ac6c886fdd73a3020c266601f58038a61']

Name

6ca0b4efe077fe05b2ae871bf50133c706c7090a54d2c3536a6c86ff454caa9a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6ca0b4efe077fe05b2ae871bf50133c706c7090a54d2c3536a6c86ff454caa9a']

Name

10c0e2afb37a24ac7732a402a4c9d854b35a382f1651d4aa2ece429b154aecb2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '10c0e2afb37a24ac7732a402a4c9d854b35a382f1651d4aa2ece429b154aecb2']

Name

http://octoberoctopus.co.za/wp-includes/sitemaps/web/

Pattern Type

stix

Pattern

[url:value = 'http://octoberoctopus.co.za/wp-includes/sitemaps/web/']

Name

e33580ae3df9d27d7cfb7b8f518a2704e55c92dd74cbbab8ef58ddfd36524cc8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e33580ae3df9d27d7cfb7b8f518a2704e55c92dd74cbbab8ef58ddfd36524cc8']

Name

www.balletmaniacs.com

Pattern Type

stix

Pattern

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

Name

fc68026b83392aa227e9adf9c71289cb51ba03427f6de67a73ae872e19ef6ff9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fc68026b83392aa227e9adf9c71289cb51ba03427f6de67a73ae872e19ef6ff9']

Name

009406c1c7c0b289a25d44dfaa8364633d9b71df5f3c7a65deec1ef00a8c2ebb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '009406c1c7c0b289a25d44dfaa8364633d9b71df5f3c7a65deec1ef00a8c2ebb']

Name

hcdh-tunisie.org

Pattern Type

stix

Pattern

[domain-name:value = 'hcdh-tunisie.org']

Name

d4ba16db7c26622d2d402cb9714331abfee891b6276d16e6c2f2132e8944cc71

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd4ba16db7c26622d2d402cb9714331abfee891b6276d16e6c2f2132e8944cc71']

Name

wekanda.tk

Pattern Type

stix

Pattern

[domain-name:value = 'wekanda.tk']

Name

cf3a7d4285d65bf8688215407bce1b51d7c6b22497f09021f0fce31cbeb78986

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cf3a7d4285d65bf8688215407bce1b51d7c6b22497f09021f0fce31cbeb78986']

Name

http://sansaispa.com/wp-includes/images/gallery/

Pattern Type

stix

Pattern

[url:value = 'http://sansaispa.com/wp-includes/images/gallery/']

Name

7a7d11adbcb740323eb52b097f535cfa5c281bf07a4d5c4afb0c5182fa4ffd1b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7a7d11adbcb740323eb52b097f535cfa5c281bf07a4d5c4afb0c5182fa4ffd1b']

Name

http://mail.lechateaudelatour.fr/MICROSOFT.EXCHANGE.MAILBOXREPLICATIONSERVICE.PROXYSERVICE/RPCWITCHERT/SYNC

Pattern Type

stix

Pattern

[url:value = 'http://mail.lechateaudelatour.fr/MICROSOFT.EXCHANGE.MAILBOXREPLICATIONSERVICE.PROXYSERVICE/RPCWITCHERT/SYNC']

Name

sanitar.ml

Pattern Type

stix

Pattern

[domain-name:value = 'sanitar.ml']

Name

00352afc7e7863530e4d68be35ae8b60261fc57560167645697b7bfc0ac0e93d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '00352afc7e7863530e4d68be35ae8b60261fc57560167645697b7bfc0ac0e93d']

Name

http://mail.kzp.bg/outlook/api/logoff.aspx

Pattern Type

stix

Pattern

[url:value = 'http://mail.kzp.bg/outlook/api/logoff.aspx']

Name

194.67.209.186

Description

ISP: NTX Technologies s.r.o. **OS:** None ---------- Hostnames: - www.api.surromusic.com - ih465921.dedic.myihor.ru - api.surromusic.com ---------- Domains: - surromusic.com - myihor.ru ---------- Services: **21:** ``` 220 ProFTPD 1.3.5 Server (Debian) [::ffff:194.67.209.186] 530 Login incorrect. 214-The following commands are recognized (* =>'s unimplemented): 214-CWD XCWD CDUP XCUP SMNT* QUIT PORT PASV 214-EPRT EPSV ALLO* RNFR RNTO DELE MDTM RMD 214-XRMD MKD XMKD PWD XPWD SIZE SYST HELP 214-NOOP FEAT OPTS AUTH* CCC* CONF* ENC* MIC* 214-PBSZ* PROT* TYPE STRU MODE RETR STOR STOU 214-APPE REST ABOR USER PASS ACCT*

REIN* LIST 214-NLST STAT SITE MLSD MLST 214 Direct comments to root@ih465921.dedic.myihor.ru 211-Features: SITE MKDIR MFF modify;UNIX.group;UNIX.mode; REST STREAM MLST modify*;perm*;size*;type*;unique*;UNIX.group*;UNIX.mode*;UNIX.owner*; UTF8 EPRT SITE SYMLINK EPSV SITE UTIME LANG ru-RU.UTF-8;ru-RU;en-US.UTF-8*;en-US MDTM SITE RMDIR TVFS SITE COPY MFMT SIZE 211 End ``` ---------- **22:** ``` SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u3 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDflJU4QUYKoCFpGkqfFQqTTHJE/GI/K1wxq7kHbhilwXj6OzvdKQvIEB1NUj+0rnxPxwkqqLqknYw9sqXiTJXqkdHjrfmkRBTEnbH7Z1cxuES2J4hdXOeGuu1kFcgX3I26SQ+SCHgaF+cwhTJCZc+PA9X0pTU3FOb59L801n+UWLHuvEtmVbJEsoNUzMVG25pSIDqKVnBj5GUzAainjwpubSaIAS4v32CoKDiMqmnH4B0Vf2ZpXFJ6jlNjeSC6zzZ2TXbNixwvtrdLlp/9qgNZlo6xG3f9R3MDeVIvj7ce3+WDyoR0Zh0hPsumkQlG1oXxvOWzKqHIC4vVb1fhFdFr Fingerprint: 22:c3:a8:d4:88:42:30:9a:51:aa:99:57:dd:64:00:88 Kex Algorithms: curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha1 Server Host Key Algorithms: ssh-rsa ssh-dss ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com chacha20-poly1305@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/1.1 403 Forbidden Server: nginx Date: Wed, 04 Jan 2023 10:54:25 GMT Content-Type: text/html Content-Length: 564 Connection: keep-alive ``` ---------- **443:** ``` HTTP/1.1 404 Not Found Server: nginx Date: Tue, 24 Jan 2023 03:45:00 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 602 Connection: keep-alive Access-Control-Allow-Origin: * ``` HEARTBLEED: 2023/01/24 03:45:07 194.67.209.186:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '194.67.209.186']

Name

bronerg.tk

Pattern Type

stix

Pattern

[domain-name:value = 'bronerg.tk']

Name

f3aaa091fdbc8772fb7bd3a81665f4d33c3b62bf98caad6fee4424654ba26429

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f3aaa091fdbc8772fb7bd3a81665f4d33c3b62bf98caad6fee4424654ba26429']

Name

2b969111dd1968d47b02d6390c92fb622cd03570b02ecf9215031ff03611a2b7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2b969111dd1968d47b02d6390c92fb622cd03570b02ecf9215031ff03611a2b7']

Name

210.48.231.182

Description

ISP: NTT PC Communications, Inc. **OS:** FreeBSD ---------- Hostnames: - ns.nutter.co.jp ---------- Domains: - nutter.co.jp ---------- Services: **21:** ``` 220 ProFTPD 1.3.5b Server (nutter-servers) [210.48.231.182] 530 Login incorrect. 214-The following commands are recognized (* =>'s unimplemented): CWD XCWD CDUP XCUP SMNT* QUIT PORT PASV EPRT EPSV ALLO* RNFR RNTO DELE MDTM RMD XRMD MKD XMKD PWD XPWD SIZE SYST HELP NOOP FEAT OPTS AUTH* CCC* CONF* ENC* MIC* PBSZ* PROT* TYPE STRU MODE RETR STOR STOU APPE REST ABOR USER PASS ACCT* REIN* LIST NLST STAT SITE MLSD MLST 214 Direct comments to root@ns.nutter.co.jp 211-Features: UTF8 EPRT EPSV LANG it-IT.UTF-8;it-IT;bg-BG.UTF-8;bg-BG;es-ES.UTF-8;es-ES;ko-KR.UTF-8;ko-KR;ja-JP.UTF-8;ja-JP;zh-CN.UTF-8;zh-CN;ru-RU.UTF-8;ru-RU;zh-TW.UTF-8;zh-TW;fr-FR.UTF-8;fr-FR;en-US.UTF-8;en-US* MDTM TVFS MFMT SIZE MFF modify;UNIX.group;UNIX.mode; REST STREAM MLST modify*;perm*;size*;type*;unique*;UNIX.group*;UNIX.mode*;UNIX.owner*; 211 End ``` ---------- **22:** ``` SSH-2.0-OpenSSH_6.6.1_hpn13v11 FreeBSD-20140420 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQC/G8ToYzZ/ 8hGSUGX2BjyWONoFjFTybsELh97nlHnqdqU1 qfSCVsmyY4eQ+VvYNcsMy/ 1Ao1Np9xUO2Es17aaxm0QmJsKMG+T0VJB4rnUFGHQbZI67GhXFbQcu ucD2e/ sh5ed9wvXAdc29OveE6uupEY5o3CpaIBuK5AaYEgkHT1wcaFIqnFYnGpVnlnXlMZbnMAQk kWFjzE+iLOSrSpsAYaR9lCtN0JvDHv/SukphHyjU668+4GFV9edepsDUDIUHVgbUFqaCm7wgxNas 03ysAo43qCYl6QMhNUnLS24PX8leto1XwgX2pnqKHwSgYqoUlZo/qZ22aAVAViKPBbM1 Fingerprint: 1c:71:9c:f5:b5:b3:03:45:e9:45:2a:b3:8d:fc:bb:93 Kex Algorithms: curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa ssh-dss ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: aes128-ctr aes192-ctr aes256-ctr arcfour256 arcfour128 chacha20-poly1305@openssh.com aes128-cbc 3des-cbc blowfish-cbc cast128-cbc aes192-cbc aes256-cbc arcfour rijndael-cbc@lysator.liu.se MAC Algorithms: hmac-md5-etm@openssh.com hmac-sha1-etm@openssh.com umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-ripemd160-etm@openssh.com hmac-sha1-96-etm@openssh.com hmac-md5-96-etm@openssh.com hmac-md5 hmac-sha1 umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-ripemd160 hmac-ripemd160@openssh.com hmac-sha1-96 hmac-md5-96 Compression Algorithms: none zlib@openssh.com ``` ---------- **25:** ``` 220 ns.nutter.co.jp ESMTP Postfix 250-ns.nutter.co.jp 250-PIPELINING 250-SIZE 102400000 250-VRFY 250-ETRN 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN ``` ---------- **110:** ``` +OK Dovecot ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING USER SASL PLAIN LOGIN . ``` ---------- **143:** ``` * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE AUTH=PLAIN AUTH=LOGIN]

Dovecot ready. * CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE SORT SORT=DISPLAY THREAD=REFERENCES THREAD=REFS MULTIAPPEND UNSELECT IDLE CHILDREN NAMESPACE UIDPLUS LIST-EXTENDED I18NLEVEL=1 CONDSTORE QRESYNC ESEARCH ESORT SEARCHRES WITHIN CONTEXT=SEARCH LIST-STATUS AUTH=PLAIN AUTH=LOGIN A001 OK Capability completed. * ID NIL A002 OK ID completed. A003 BAD Error in IMAP command received by server. * BYE Logging out A004 OK Logout completed. ``` ---------- **587:** ``` 220 ns.nutter.co.jp ESMTP Postfix 250-ns.nutter.co.jp 250-PIPELINING 250-SIZE 102400000 250-VRFY 250-ETRN 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN ``` ---------- **873:** ``` ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '210.48.231.182']

Name

166b1fb3d34b32f1807c710aaa435d181aedbded1e7b4539ffa931c2b2cdd405

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '166b1fb3d34b32f1807c710aaa435d181aedbded1e7b4539ffa931c2b2cdd405']

Name

030cbd1a51f8583ccfc3fa38a28a5550dc1c84c05d6c0f5eb887d13dedf1da01

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '030cbd1a51f8583ccfc3fa38a28a5550dc1c84c05d6c0f5eb887d13dedf1da01']

Name

29b1da7b17a7ba3e730e6927058d0554a8bc81bdef88e364097fab0bb1950edc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '29b1da7b17a7ba3e730e6927058d0554a8bc81bdef88e364097fab0bb1950edc']

Name

crusider.tk

Pattern Type

stix

Pattern

[domain-name:value = 'crusider.tk']

Name

gaismustudija.lv

Pattern Type
stix
Pattern
[domain-name:value = 'gaismustudija.lv']
Name
mail.aet.in.ua
Pattern Type
stix
Pattern
[hostname:value = 'mail.aet.in.ua']
Name
manager.surro.am
Pattern Type
stix
Pattern
[hostname:value = 'manager.surro.am']

Intrusion-Set

Name
Turla

Description
[Turla](https://attack.mitre.org/groups/G0010) is a Russian-based threat group that has infected victims in over 45 countries, spanning a range of industries including government, embassies, military, education, research and pharmaceutical companies since 2004. Heightened activity was seen in mid-2015. [Turla](https://attack.mitre.org/groups/G0010) is known for conducting watering hole and spearphishing campaigns and leveraging in-house tools and malware. [Turla](https://attack.mitre.org/groups/G0010)'s espionage platform is mainly used against Windows machines, but has also been seen used against macOS and Linux machines.(Citation: Kaspersky Turla)(Citation: ESET Gazer Aug 2017) (Citation: CrowdStrike VENOMOUS BEAR)(Citation: ESET Turla Mosquito Jan 2018)

Malware

Name
QUIETCANARY
Name
HyperStack - S0537
Name
Kazuar
Description
[Kazuar](https://attack.mitre.org/software/S0265) is a fully featured, multi-platform backdoor Trojan written using the Microsoft .NET framework. (Citation: Unit 42 Kazuar May 2017)
Name
KopiLuwak
Name
Snake
Name

Crutch - S0538
Name
Capibar
Name
ComRAT - S0126
Name
TinyTurla - S0668

Domain-Name

Value
gaismustudija.lv
bronerg.tk
sansaispa.com
sanitar.ml
hcdh-tunisie.org
octoberoctopus.co.za
crusider.tk
branter.tk
duke6.tk
wekanda.tk
lakihelppi.com

StixFile

Value
7d5794ad91351c7c5d7fbad8e83e3b71a09baac65fb09ca75d8d18339d24a46f
8d9bb878a18b2b7ef558504e78a59eb644f83a63679658533ff8accf0b85fda3
030cbd1a51f8583ccfc3fa38a28a5550dc1c84c05d6c0f5eb887d13dedf1da01
8490daab736aa638b500b27c962a8250bbb8615ae1c68ef77494875ac9d2ada2
cd4c2e85213c96f79ddda564242efec3b970eded8c59f1f6f4d9a420eb8f1858
b51105c56d1bf8f98b7e924aa5caded8322d037745a128781fa0bc23841d1e70
29b1da7b17a7ba3e730e6927058d0554a8bc81bdef88e364097fab0bb1950edc
44d6d67b5328a4d73f72d8a0f9d39fe4bb6539609f90f169483936a8b3b88316
b262292e049ee75d235164df98fa8ed09a9e2a30c5432623856bafd4bd44d801
493e5fae191950b901764868b065ddddffa4f4c9b497022ee2f998b4a94f0fc2
166b1fb3d34b32f1807c710aaa435d181aedbded1e7b4539ffa931c2b2cdd405
3f94b20cb7f4ff55207660649ebbb02679c991fe03efbcb0bd3840fc7f0bd527
7a7d11adbcb740323eb52b097f535cfa5c281bf07a4d5c4afb0c5182fa4ffd1b

b93484683014aca8e909c9b5648d8f0ac21a45d0c193f6ca40f0b01d2464c1c4

187bf95439da038c1bc291619507ff5e426d250709fa5e3eda7fda99e1c9854c

d4ba16db7c26622d2d402cb9714331abfee891b6276d16e6c2f2132e8944cc71

0fc624aa9656a8bc21731bfc47fd7780da38a7e8ad7baf1529ccd70a5bb07852

16860fc685ea0dee91e65e253062153ac6c886fdd73a3020c266601f58038a61

6536b6b50aa1f6899ffa90aaf4b1b67c0ae0f6c0441016f5308b37c12141c61d

2b969111dd1968d47b02d6390c92fb622cd03570b02ecf9215031ff03611a2b7

009406c1c7c0b289a25d44dfaa8364633d9b71df5f3c7a65deec1ef00a8c2ebb

64e8744b39e15b76311733014327311acd77330f8a135132f020eac78199ac8a

87663affd147065d08d4fe76d9a18b0d7d85fab68cf9f5ac96cfdfff3f27ffd2

00352afc7e7863530e4d68be35ae8b60261fc57560167645697b7bfc0ac0e93d

bf6f30673cf771d52d589865675a293dc5c3668a956d0c2fc0d9403424d429b2

20691ff3c9474cfd7bf6fa3f8720eb7326e6f87f64a1f190861589c1e7397fa5

046f11a6c561e46e6bf199ab7f50e74a4d2aaead68cdbd6ce44b37b5b4964758

6ca0b4efe077fe05b2ae871bf50133c706c7090a54d2c3536a6c86ff454caa9a

134919151466c9292bdcb7c24c32c841a5183d880072b0ad5e8b3a3a830afef8

a3170c32c09fc85cdda778a5c20a3dab144b6d1dd9996ba8340866e0081c7642

f3aaa091fdbc8772fb7bd3a81665f4d33c3b62bf98caad6fee4424654ba26429

cf3a7d4285d65bf8688215407bce1b51d7c6b22497f09021f0fce31cbeb78986

0010ccb822538d1881c61be874af49382c44b6c9cb665081cf0f672cbed5b6a5

fc68026b83392aa227e9adf9c71289cb51ba03427f6de67a73ae872e19ef6ff9

e33580ae3df9d27d7cfb7b8f518a2704e55c92dd74cbbab8ef58ddfd36524cc8

29314f3cd73b81eda7bd90c66f659235e6bb900e499c9cc7057d10a9083a0b94

1950d2e706fbc6263d376c0c4f16bd5acfd543248ee072657ba3dd62da8427eb

10c0e2afb37a24ac7732a402a4c9d854b35a382f1651d4aa2ece429b154aecb2

ba2c8df04bcba5c3cfd343a59d8b59b76779e6c27eb27b7ac73ded97e08f0f39

Hostname

Value
www.gallen.fi
www.bombheros.com
www.pierreagencement.fr
mail.aet.in.ua
mail.arlingtonhousing.us
mail.lebsack.de
mail.lechateaudelatour.fr
www.simplifiedhomesales.com
www.balletmaniacs.com
manager.surro.am
mtsoft.hol.es
mail.kzp.bg
www.berlinguas.com

IPv4-Addr

Value
194.67.209.186
210.48.231.182
197.168.0.247

Url

Value
http://sansaispa.com/wp-includes/images/gallery/
http://www.bombheros.com/wp-content/languages/index.php
http://mail.aet.in.ua/outlook/api/logoff.aspx
http://mail.lebsack.de/MICROSOFT.EXCHANGE.MAILBOXREPLICATIONSERVICE.PROXYSERVICE/RPCWITCHERT/SYNC
http://www.pierreagencement.fr/wp-content/languages/index.php
http://mtsoft.hol.es/wp-content/gallery/
http://octoberoctopus.co.za/wp-includes/sitemaps/web/
http://mail.lechateaudelatour.fr/MICROSOFT.EXCHANGE.MAILBOXREPLICATIONSERVICE.PROXYSERVICE/RPCWITCHERT/SYNC
http://mail.arlingtonhousing.us/outlook/api/logoff.aspx
http://mail.kzp.bg/outlook/api/logoff.aspx
http://www.simplifiedhomesales.com/wp-includes/images/index.php
http://mail.numina.md/owa/scripts/logon.aspx

External References

- https://otx.alienvault.com/pulse/650809050ea516cd84c8ef74
- https://unit42.paloaltonetworks.com/turla-pensive-ursa-threat-assessment/