Oct 15 2023

NETMANAGEIT

Intelligence Report

Stayin’ Alive – Targeted Attacks Against Telecoms and Government Ministries in Asia

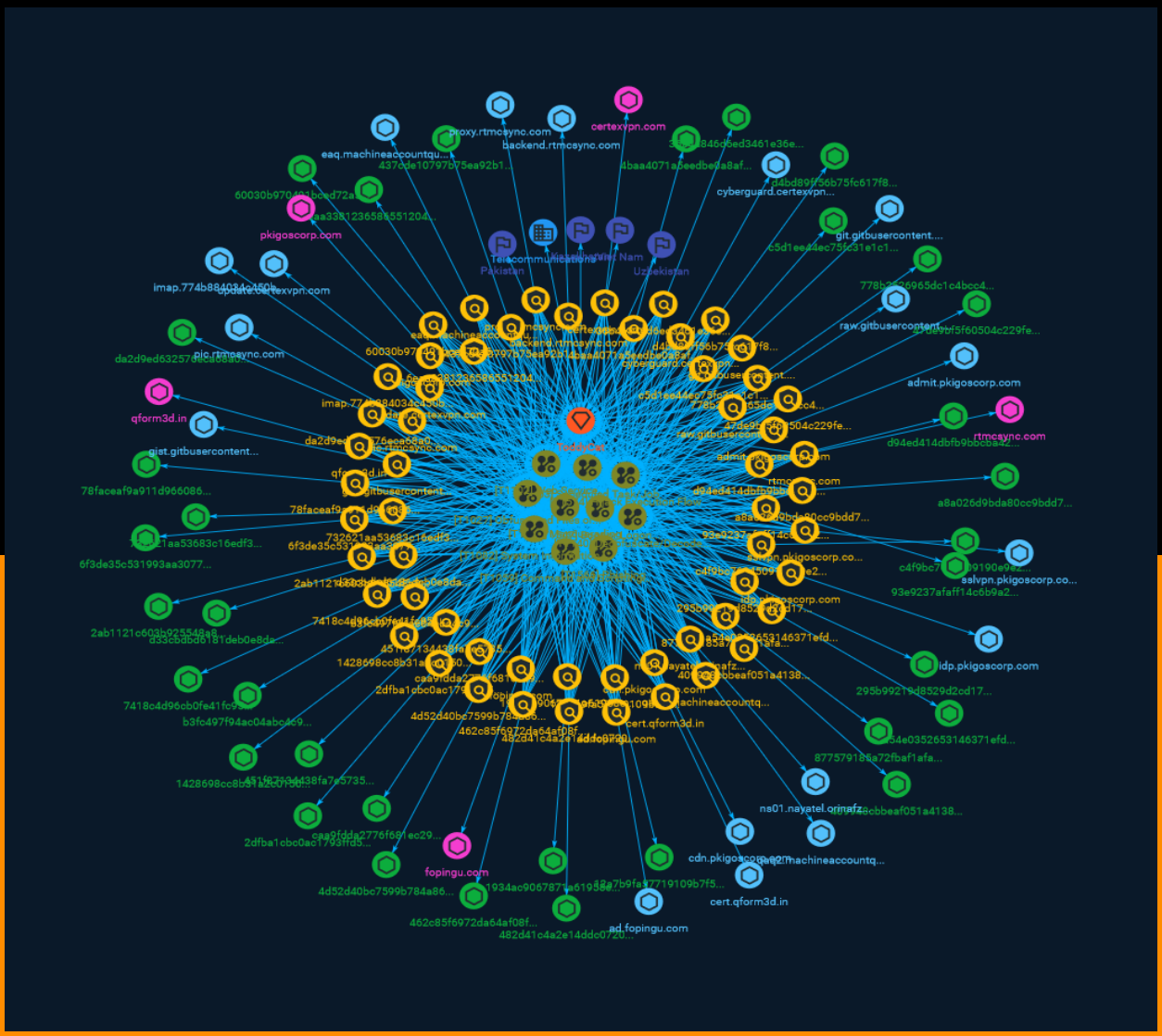

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The “Stayin’ Alive” campaign consists of mostly downloaders and loaders, some of which are used as an initial infection vector against high-profile Asian organizations. The first downloader found called CurKeep, targeted Vietnam, Uzbekistan, and Kazakhstan. As we conducted our analysis, we realized that this campaign is part of a much wider campaign targeting the region.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Boot or Logon Autostart Execution
ID
T1547
Description
Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.
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

Scheduled Task/Job

ID

T1053

Description

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.(Citation: TechNet Task Scheduler Security) Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process. (Citation: ProofPoint Serpent)

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. 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 malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as 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) 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) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit.

This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

Hijack Execution Flow

ID

T1574

Description

Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution. There are many ways an adversary may hijack the flow of execution, including by manipulating how the operating system locates programs to be executed. How the operating system locates libraries to be used by a program can also be intercepted. Locations where the operating system looks for programs/resources, such as file directories and in the case of Windows the Registry, could also be poisoned to include malicious payloads.

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

Web Service

ID

T1102

Description

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection. Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

Name

System Information Discovery

ID

T1082

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. `show version`).(Citation: US-CERT-TA18-106A) [System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)

Sector

Name
Telecommunications
Description
Private and public entities involved in the production, transport and dissemination of information and communication signals.

Indicator

Name
4baa4071a5eedbe0a8afa1059f7732e5cde0433dd0425e075721dd2cdec9d70d
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '4baa4071a5eedbe0a8afa1059f7732e5cde0433dd0425e075721dd2cdec9d70d']
Name
cdn.pkigoscorp.com
Pattern Type
stix
Pattern
[hostname:value = 'cdn.pkigoscorp.com']
Name

pic.rtmcsync.com

Pattern Type

stix

Pattern

[hostname:value = 'pic.rtmcsync.com']

Name

d94ed414dbfb9bbcba42e3bf2db3b76eb8172b03133d1745d6abcde6f9edbaa7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd94ed414dbfb9bbcba42e3bf2db3b76eb8172b03133d1745d6abcde6f9edbaa7']

Name

caa9fdda2776f681ec294ffeded04723107cf754a2889c3fbb5bc7c743d897c1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'caa9fdda2776f681ec294ffeded04723107cf754a2889c3fbb5bc7c743d897c1']

Name
backend.rtmcsync.com
Pattern Type
stix
Pattern
[hostname:value = 'backend.rtmcsync.com']
Name
877579185a72fbaf1afa78d3c50dbab187780d545d5375ba4c29147083176697
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '877579185a72fbaf1afa78d3c50dbab187780d545d5375ba4c29147083176697']
Name
gist.gitbusercontent.com
Pattern Type
stix
Pattern

[hostname:value = 'gist.gitbusercontent.com']

Name

778b2526965dc1c4bcc401d0ae92037122e7e7f2c41f042f95b59a7f0fe6f30e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '778b2526965dc1c4bcc401d0ae92037122e7e7f2c41f042f95b59a7f0fe6f30e']

Name

12a7b9fa57719109b7f5d081cbe032320a59a7d57eef2dcd2cd4fe2b909162dc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '12a7b9fa57719109b7f5d081cbe032320a59a7d57eef2dcd2cd4fe2b909162dc']

Name

update.certexvpn.com

Pattern Type

stix

Pattern

[hostname:value = 'update.certexvpn.com']

Name

93e9237afaff14c6b9a24cf7275e9d66bc95af8a0cc93db2a68b47cbbca4c347

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '93e9237afaff14c6b9a24cf7275e9d66bc95af8a0cc93db2a68b47cbbca4c347']

Name

451f87134438fa7e5735a865989072e7bab4858ca0b1e921224ed27dea0226b0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '451f87134438fa7e5735a865989072e7bab4858ca0b1e921224ed27dea0226b0']

Name

proxy.rtmcsync.com

Pattern Type

stix

Pattern

[hostname:value = 'proxy.rtmcsync.com']

Name

ns01.nayatel.orinafz.com

Pattern Type

stix

Pattern

[hostname:value = 'ns01.nayatel.orinafz.com']

Name

732621aa53683c16edf3959dfe9d93de5359c431c130784b31d4a598fbbd80a9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '732621aa53683c16edf3959dfe9d93de5359c431c130784b31d4a598fbbd80a9']

Name

raw.gitbusercontent.com

Pattern Type

stix

Pattern

[hostname:value = 'raw.gitbusercontent.com']

Name

fopingu.com

Pattern Type

stix

Pattern

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

Name

6eaa3381236586551204402 0bc4b95079a1cc2ddc26cdadf24a9ff76c81b1746

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6eaa3381236586551204402 0bc4b95079a1cc2ddc26cdadf24a9ff76c81b1746']

Name

c4f9bc7624509190e9e2a690daeff5ac9e944f094b51781734b83a364ae038d0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c4f9bc7624509190e9e2a690daeff5ac9e944f094b51781734b83a364ae038d0']

Name

d33cbdbd6181deb0e8da9c9e6fb8795e98478d9608ab187e5b8809bed6b2e5c4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd33cbdbd6181deb0e8da9c9e6fb8795e98478d9608ab187e5b8809bed6b2e5c4']

Name

c5d1ee44ec75fc31e1c11fbf7a70ed7ca8c782099abfde15ecaa1b1edaf180ac

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c5d1ee44ec75fc31e1c11fbf7a70ed7ca8c782099abfde15ecaa1b1edaf180ac']

Name

ad.fopingu.com

Pattern Type

stix

Pattern

[hostname:value = 'ad.fopingu.com']

Name

da2d9ed632576eca68a0c6d8d5afd383a1d811c369012f0d7fb52cd06da8c9b9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'da2d9ed632576eca68a0c6d8d5afd383a1d811c369012f0d7fb52cd06da8c9b9']

Name

rtmcsync.com

Pattern Type

stix

Pattern

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

Name

2dfba1cbc0ac1793ffd591c88024fab598a3f6a91756a2ea79f84f1601a0f1ed

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2dfba1cbc0ac1793ffd591c88024fab598a3f6a91756a2ea79f84f1601a0f1ed']

Name

437cde10797b75ea92b1b68eb887972fe43b434db3ed67b756e01698cce69b4a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '437cde10797b75ea92b1b68eb887972fe43b434db3ed67b756e01698cce69b4a']

Name

a54e0352653146371efd727ca00110577f8e750e92101462e246f99d435b6172

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a54e0352653146371efd727ca00110577f8e750e92101462e246f99d435b6172']

Name

6f3de35c531993aa307729e2046ff7aa672f5058b7e0fc6557bbd4c500fb46e7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6f3de35c531993aa307729e2046ff7aa672f5058b7e0fc6557bbd4c500fb46e7']

Name

git.gitbusercontent.com

Pattern Type

stix

Pattern

[hostname:value = 'git.gitbusercontent.com']

Name

1934ac9067871a61958e3e96ea5daa227900b7683fce67a1bf1c24beff77d75a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1934ac9067871a61958e3e96ea5daa227900b7683fce67a1bf1c24beff77d75a']

Name

pkigoscorp.com

Pattern Type

stix

Pattern

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

Name

sslvpn.pkigoscorp.com

Pattern Type

stix

Pattern

[hostname:value = 'sslvpn.pkigoscorp.com']

Name

b3fc497f94ac04abc4c9a6f23ab142fdc2387c520ce5c6fdae1b511793bc6ba2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b3fc497f94ac04abc4c9a6f23ab142fdc2387c520ce5c6fdae1b511793bc6ba2']

Name

cyberguard.certexvpn.com

Pattern Type

stix

Pattern

[hostname:value = 'cyberguard.certexvpn.com']

Name

qaq2.machineaccountquota.com

Pattern Type

stix

Pattern

[hostname:value = 'qaq2.machineaccountquota.com']

Name
qform3d.in
Pattern Type
stix
Pattern
[domain-name:value = 'qform3d.in']
Name
admit.pkigoscorp.com
Pattern Type
stix
Pattern
[hostname:value = 'admit.pkigoscorp.com']
Name
4d52d40bc7599b784a86a000ff436527babc46c5de737e19ded265416b4977c6
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '4d52d40bc7599b784a86a000ff436527babc46c5de737e19ded265416b4977c6']

Name

eaq.machineaccountquota.com

Pattern Type

stix

Pattern

[hostname:value = 'eaq.machineaccountquota.com']

Name

295b99219d8529d2cd17b71a7947d370809f4e1a3094a74a31da6e30aa39e719

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '295b99219d8529d2cd17b71a7947d370809f4e1a3094a74a31da6e30aa39e719']

Name

2ab1121c603b925548a823fa18193896cd24d186e08957393e6a34d697aed782

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2ab1121c603b925548a823fa18193896cd24d186e08957393e6a34d697aed782']

Name

d4bd89ff56b75fc617f83eb858b6dbce7b36376889b07fa0c2417322ca361c30

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd4bd89ff56b75fc617f83eb858b6dbce7b36376889b07fa0c2417322ca361c30']

Name

482d41c4a2e14ddc072087a1b96f6e34ffda2bfc85819e21f15c97220825e651

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '482d41c4a2e14ddc072087a1b96f6e34ffda2bfc85819e21f15c97220825e651']

Name

imap.774b884034c450b.com

Pattern Type

stix

Pattern

[hostname:value = 'imap.774b884034c450b.com']

Name

a8a026d9bda80cc9bdd778a6ea8c88edcb2d657dc481952913bbdb5f2bfc11c9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a8a026d9bda80cc9bdd778a6ea8c88edcb2d657dc481952913bbdb5f2bfc11c9']

Name

1428698cc8b31a2c0150065af7b615ef2374ea3438b0a82f2efcff306b43cee6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1428698cc8b31a2c0150065af7b615ef2374ea3438b0a82f2efcff306b43cee6']

Name

certexvpn.com

Pattern Type

stix

Pattern

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

Name

409948cbbeaf051a41385d2e2bc32fc1e59789986852e608124b201d079e5c3c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '409948cbbeaf051a41385d2e2bc32fc1e59789986852e608124b201d079e5c3c']

Name

78faceaf9a911d966086071ff085f2d5c2713b58446d48e0db1ad40974bb15cd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '78faceaf9a911d966086071ff085f2d5c2713b58446d48e0db1ad40974bb15cd']

Name

47de9bf5f60504c229fe9f727aa59ba5c34d173a23af70822541a9e485abe391

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '47de9bf5f60504c229fe9f727aa59ba5c34d173a23af70822541a9e485abe391']

Name

462c85f6972da64af08f52a4c2f3a03bcd40fdf29b29b01631bff643cd9d906a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '462c85f6972da64af08f52a4c2f3a03bcd40fdf29b29b01631bff643cd9d906a']

Name

60030b970491bced72a56c9dde09a1d2260becfbf80a2b0d217a0b913e781c3a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '60030b970491bced72a56c9dde09a1d2260becfbf80a2b0d217a0b913e781c3a']

Name

idp.pkigoscorp.com

Pattern Type

stix

Pattern

[hostname:value = 'idp.pkigoscorp.com']

Name

7418c4d96cb0fe41fc95c0a27d2364ac45eb749d7edbe0ab339ea954f86abf9e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7418c4d96cb0fe41fc95c0a27d2364ac45eb749d7edbe0ab339ea954f86abf9e']

Name

36b4a846d6ed3461e36ed9f4c03fb4548397659ef0a46219695666266eba1652

Pattern Type

stix

Pattern
[file:hashes.'SHA-256' = '36b4a846d6ed3461e36ed9f4c03fb4548397659ef0a46219695666266eba1652']
Name
cert.qform3d.in
Pattern Type
stix
Pattern
[hostname:value = 'cert.qform3d.in']

Intrusion-Set

Name
ToddyCat

Country

Name
Uzbekistan
Name
Kazakhstan
Name
Viet Nam
Name
Pakistan

Domain-Name

Value
pkigoscorp.com
fopingu.com
qform3d.in
certexvpn.com
rtmcsync.com

StixFile

Value
c4f9bc7624509190e9e2a690daeff5ac9e944f094b51781734b83a364ae038d0
6eaa33812365865512044020bc4b95079a1cc2ddc26cdadf24a9ff76c81b1746
da2d9ed632576eca68a0c6d8d5afd383a1d811c369012f0d7fb52cd06da8c9b9
47de9bf5f60504c229fe9f727aa59ba5c34d173a23af70822541a9e485abe391
295b99219d8529d2cd17b71a7947d370809f4e1a3094a74a31da6e30aa39e719
b3fc497f94ac04abc4c9a6f23ab142fdc2387c520ce5c6fdae1b511793bc6ba2
451f87134438fa7e5735a865989072e7bab4858ca0b1e921224ed27dea0226b0
60030b970491bced72a56c9dde09a1d2260becfbf80a2b0d217a0b913e781c3a
4d52d40bc7599b784a86a000ff436527babc46c5de737e19ded265416b4977c6
877579185a72fbaf1afa78d3c50dbab187780d545d5375ba4c29147083176697
a8a026d9bda80cc9bdd778a6ea8c88edcb2d657dc481952913bbdb5f2bfc11c9
7418c4d96cb0fe41fc95c0a27d2364ac45eb749d7edbe0ab339ea954f86abf9e
4baa4071a5eedbe0a8afa1059f7732e5cde0433dd0425e075721dd2cdec9d70d

1934ac9067871a61958e3e96ea5daa227900b7683fce67a1bf1c24beff77d75a

6f3de35c531993aa307729e2046ff7aa672f5058b7e0fc6557bbd4c500fb46e7

36b4a846d6ed3461e36ed9f4c03fb4548397659ef0a46219695666266eba1652

462c85f6972da64af08f52a4c2f3a03bcd40fdf29b29b01631bff643cd9d906a

d4bd89ff56b75fc617f83eb858b6dbce7b36376889b07fa0c2417322ca361c30

2dfba1cbc0ac1793ffd591c88024fab598a3f6a91756a2ea79f84f1601a0f1ed

d33cbdbd6181deb0e8da9c9e6fb8795e98478d9608ab187e5b8809bed6b2e5c4

482d41c4a2e14ddc072087a1b96f6e34ffda2bfc85819e21f15c97220825e651

12a7b9fa57719109b7f5d081cbe032320a59a7d57eef2dcd2cd4fe2b909162dc

732621aa53683c16edf3959dfe9d93de5359c431c130784b31d4a598fbbd80a9

437cde10797b75ea92b1b68eb887972fe43b434db3ed67b756e01698cce69b4a

778b2526965dc1c4bcc401d0ae92037122e7e7f2c41f042f95b59a7f0fe6f30e

93e9237afaff14c6b9a24cf7275e9d66bc95af8a0cc93db2a68b47cbbca4c347

1428698cc8b31a2c0150065af7b615ef2374ea3438b0a82f2efcff306b43cee6

c5d1ee44ec75fc31e1c11fbf7a70ed7ca8c782099abfde15ecaa1b1edaf180ac

409948cbbeaf051a41385d2e2bc32fc1e59789986852e608124b201d079e5c3c

78faceaf9a911d966086071ff085f2d5c2713b58446d48e0db1ad40974bb15cd

caa9fdda2776f681ec294ffeded04723107cf754a2889c3fbb5bc7c743d897c1

d94ed414dbfb9bbcba42e3bf2db3b76eb8172b03133d1745d6abcde6f9edbaa7

a54e0352653146371efd727ca00110577f8e750e92101462e246f99d435b6172

2ab1121c603b925548a823fa18193896cd24d186e08957393e6a34d697aed782

Hostname

Value
raw.gitbusercontent.com
git.gitbusercontent.com
ns01.nayatel.orinafz.com
ad.fopingu.com
backend.rtmcsync.com
cdn.pkigoscorp.com
qaq2.machineaccountquota.com
sslvpn.pkigoscorp.com
imap.774b884034c450b.com
pic.rtmcsync.com
update.certexvpn.com
proxy.rtmcsync.com
admit.pkigoscorp.com

idp.pkigoscorp.com

gist.gitbusercontent.com

cert.qform3d.in

eaq.machineaccountquota.com

cyberguard.certexvpn.com

External References

- https://otx.alienvault.com/pulse/65284bd1d98ea20d7f6ef797
- https://research.checkpoint.com/2023/stayin-alive-targeted-attacks-against-telecoms-and-government-ministries-in-asia/