Mar 19 2024

NETMANAGEIT

Intelligence Report

Ongoing ITG05 operations leverage evolving malware arsenal in global campaigns

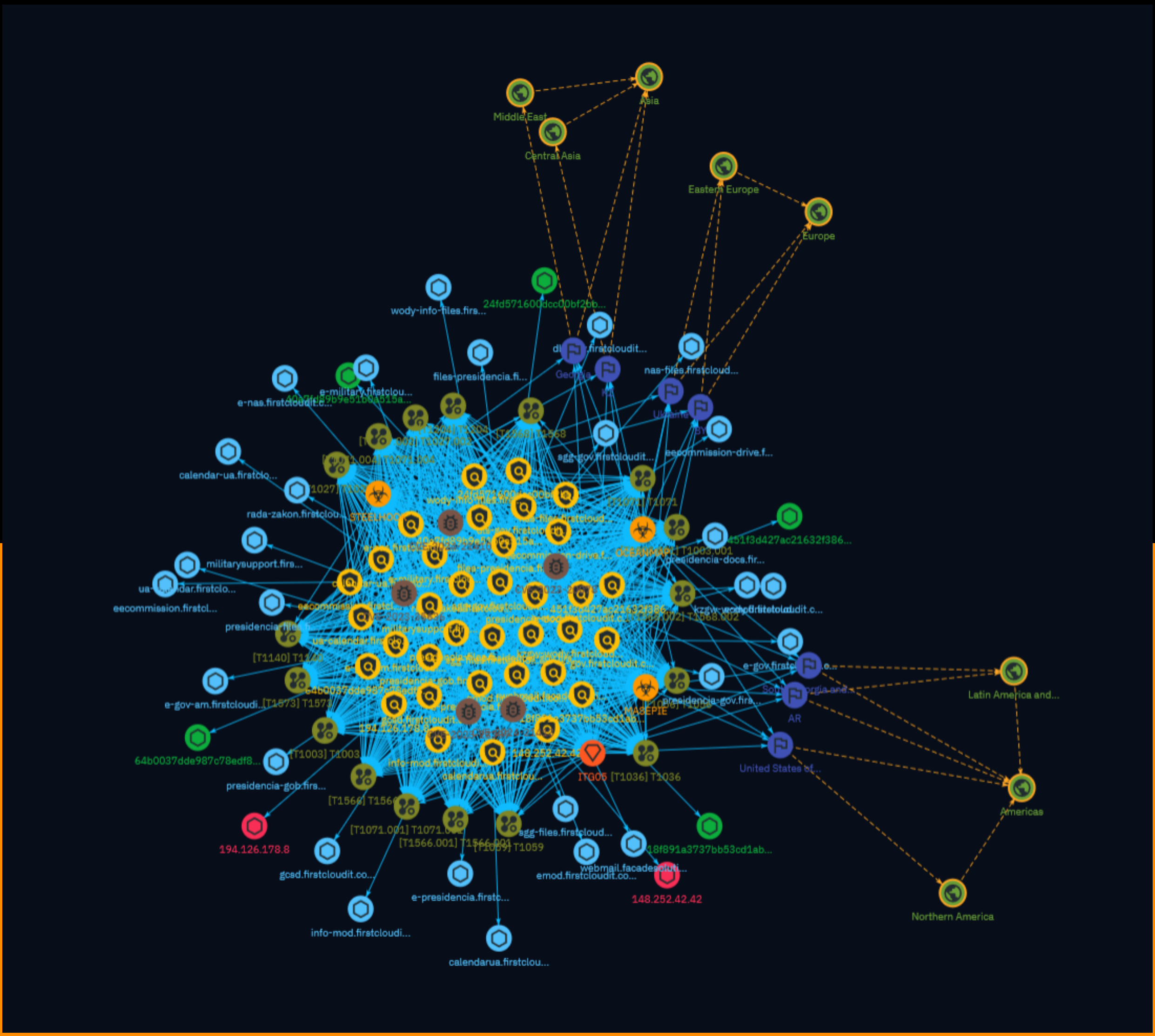

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A recent report details that the threat actor group ITG05 has been conducting phishing campaigns targeting entities in Europe, the Caucasus, Central Asia, and the Americas since late 2023. The group has introduced new techniques like search-ms protocol abuse and WebDAV servers to deploy backdoors like MASEPIE and OCEANMAP. ITG05 continues evolving tactics to steal sensitive data.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

sgg-gov.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'sgg-gov.firstcloudit.com']

Name

sgg-files.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'sgg-files.firstcloudit.com']

Name

rada-zakon.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'rada-zakon.firstcloudit.com']

Name

presidencia-gov.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'presidencia-gov.firstcloudit.com']

Name

presidencia-gob.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'presidencia-gob.firstcloudit.com']

Name

presidencia-docs.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'presidencia-docs.firstcloudit.com']

Name

presidencia-files.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'presidencia-files.firstcloudit.com']

Name

militarysupport.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'militarysupport.firstcloudit.com']

Name

kzgw-wody.firstcloudit.com

Pattern Type
stix

Pattern
[hostname:value = 'kzgw-wody.firstcloudit.com']

Name
gcsd.firstcloudit.com

Pattern Type
stix

Pattern
[hostname:value = 'gcsd.firstcloudit.com']

Name
files-presidencia.firstcloudit.com

Pattern Type
stix

Pattern
[hostname:value = 'files-presidencia.firstcloudit.com']

Name
emod.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'emod.firstcloudit.com']

Name

eecommission.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'eecommission.firstcloudit.com']

Name

eecommission-drive.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'eecommission-drive.firstcloudit.com']

Name

e-presidencia.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'e-presidencia.firstcloudit.com']

Name

e-military.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'e-military.firstcloudit.com']

Name

e-gov.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'e-gov.firstcloudit.com']

Name

e-gov-am.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'e-gov-am.firstcloudit.com']

Name

dls-gov.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'dls-gov.firstcloudit.com']

Name

calendarua.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'calendarua.firstcloudit.com']

Name

calendar-ua.firstcloudit.com

Pattern Type
stix

Pattern
[hostname:value = 'calendar-ua.firstcloudit.com']

Name
451f3d427ac21632f38619ef96dece25798918866d44fe82ff1ed30996f998dc

Pattern Type
stix

Pattern
[file:hashes.'SHA-256' = '451f3d427ac21632f38619ef96dece25798918866d44fe82ff1ed30996f998dc']

Name
64b0037dde987c78edf807a1bd7f09cdfac072ec2a59954cc4918828b7e608a3

Pattern Type
stix

Pattern
[file:hashes.'SHA-256' = '64b0037dde987c78edf807a1bd7f09cdfac072ec2a59954cc4918828b7e608a3']

Name

40a7fd89b9e51b0a515ac2355036d203357be90a2200b9c506b95c12db54c7aa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '40a7fd89b9e51b0a515ac2355036d203357be90a2200b9c506b95c12db54c7aa']

Name

148.252.42.42

Description

- **Zip Code:** N/A - **ISP:** Marston's Telecoms - **ASN:** 61124 - **Organization:** Marston's Telecoms - **Is Crawler:** False - **Timezone:** Europe/London - **Mobile:** False - **Host:** 148.252.42.42 - **Proxy:** False - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** GB - **Region:** England - **City:** Chiswick - **Latitude:** 51.49359894 - **Longitude:** -0.25830001

Pattern Type

stix

Pattern

[ipv4-addr:value = '148.252.42.42']

Name

wody-info-files.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'wody-info-files.firstcloudit.com']

Name

webmail.facadesolutionsuae.com

Pattern Type

stix

Pattern

[hostname:value = 'webmail.facadesolutionsuae.com']

Name

ua-calendar.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'ua-calendar.firstcloudit.com']

Name

nas-files.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'nas-files.firstcloudit.com']

Name

info-mod.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'info-mod.firstcloudit.com']

Name

e-nas.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'e-nas.firstcloudit.com']

Name

e-mod.firstcloudit.com

Pattern Type

stix

Pattern

[hostname:value = 'e-mod.firstcloudit.com']

Name

194.126.178.8

Description

ISP: Eurofiber France SAS **OS:** None ------------------------- Hostnames: ------------------------- Domains: ------------------------- Services: **80:** ``` HTTP/1.1 404 Not Found Date: Mon, 18 Dec 2023 09:32:20 GMT Server: Apache/2.2.22 (Debian) Vary: Accept-Encoding Content-Length: 277 Content-Type: text/html; charset=iso-8859-1 ``` ------------------ **123:** ``` NTP protocolversion: 3 stratum: 3 leap: 0 precision: -21 rootdelay: 0.0392761230469 rootdisp: 0.0702514648438 refid: 1379946970 reftime: 3911648811.53 poll: 3 ``` ------------------ **161:** ``` SNMP: Versions: 3 Engine Boots: 2 Engineid Data: 80001f888006d5f2d354ef7c2c Enterprise: 8072 Engine Time: 278 days, 3:03:14 ``` ------------------ **179:** ``` ``` ------------------ **2222:** ``` SSH-2.0-OpenSSH_6.7p2 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDrpPewRZeln62TAlAr8DdjixIsVCe+i6myr8yFjcY4ki1pwpq7BW8JFD0xtjVqIBijvDgNnGwDk+vPyx+AJbdnvv544lT9qYcg2R5wbVJ+NzgMWLfSoWcxjo7icm6aTmlaEYlQRt8KB3lZsJeLgJS1/jzV3tYYMpwD9Z1KC2TCwkIh4iptWxCTbcFXv82kcuDwi79uhznpuniuWkwFqAoafvFT7qBqu94w5uf8L3njXAmw6OQRxftI1SlzciZnjkinsz/kNvhYWius1OjsiSYyjZoKf0c2ViFagLMc4TV+rMTmO2vt1PK5B2QfT0e3Qjd9y9uI6QM0mqozXJfYnfBr Fingerprint: f5:d1:52:6d:e4:e1:8d:c4:dd:be:04:69:c5:38:3a:19 Kex Algorithms: 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 Encryption Algorithms: aes128-ctr aes192-ctr aes256-ctr arcfour256 arcfour128 aes128-cbc 3des-cbc blowfish-cbc cast128-cbc aes192-cbc aes256-cbc arcfour rijndael-cbc@lysator.liu.se MAC Algorithms: hmac-md5 hmac-sha1 umac-64@openssh.com hmac-sha2-256 hmac-sha2-256-96 hmac-sha2-512 hmac-sha2-512-96 hmac-ripemd160 hmac-ripemd160@openssh.com hmac-sha1-96 hmac-md5-96 Compression Algorithms: none zlib@openssh.com ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '194.126.178.8']

Name

24fd571600dcc00bf2bb8577c7e4fd67275f7d19d852b909395bebcbb1274e04

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '24fd571600dcc00bf2bb8577c7e4fd67275f7d19d852b909395bebcbb1274e04']

Name

18f891a3737bb53cd1ab451e2140654a376a43b2d75f6695f3133d47a41952b6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '18f891a3737bb53cd1ab451e2140654a376a43b2d75f6695f3133d47a41952b6']

Vulnerability

Name

CVE-2024-21413

Name

CVE-2023-35636

Name

CVE-2023-20078

Name

CVE-2024-21410

Description

Microsoft Exchange Server contains an unspecified vulnerability that allows for privilege escalation.

Name

CVE-2023-23397

Description

Microsoft Office Outlook contains a privilege escalation vulnerability that allows for a NTLM Relay attack against another service to authenticate as the user.

Intrusion-Set

Name
ITG05

Malware

Name
MASEPIE

Name
STEELHOOK

Name
OCEANMAP

Attack-Pattern

Name
T1071.001
ID
T1071.001
Description
Adversaries may communicate using application layer protocols associated with web traffic 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. Protocols such as HTTP/S(Citation: CrowdStrike Putter Panda) and WebSocket(Citation: Brazking-Websockets) that carry web traffic may be very common in environments. HTTP/S packets have many fields and headers in which data can be concealed. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.
Name
T1027.002
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)

Name

T1056

ID

T1056

Description

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

Name

T1573

ID

T1573

Description

Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if secret keys are encoded and/or generated within malware samples/configuration files.

Name

T1568

ID

T1568

Description

Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations. This may be achieved by using malware that shares a common algorithm with the infrastructure the adversary uses to receive the malware's communications. These calculations can be used to dynamically adjust parameters such as the domain name, IP address, or port number the malware uses for command and control. Adversaries may use dynamic resolution for the purpose of [Fallback Channels](https://attack.mitre.org/techniques/T1008). When contact is lost with the primary command and control server malware may employ dynamic resolution as a means to reestablishing command and control.(Citation: Talos CCleanup 2017)(Citation: FireEye POSHSPY April 2017)(Citation: ESET Sednit 2017 Activity)

Name

T1059

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

T1027

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

T1003.001

ID

T1003.001

Description

Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct [Lateral Movement](https://attack.mitre.org/tactics/TA0008) using [Use Alternate Authentication Material](https://attack.mitre.org/techniques/T1550). As well as in-memory techniques, the LSASS process memory can be dumped from the target host and analyzed on a local system. For example, on the target host use procdump: * `procdump -ma lsass.exe lsass_dump` Locally, mimikatz can be run using: * `sekurlsa::Minidump lsassdump.dmp` * `sekurlsa::logonPasswords` Built-in Windows tools such as comsvcs.dll can also be used: * `rundll32.exe C:\Windows\System32\comsvcs.dll MiniDump PID lsass.dmp full`(Citation: Volexity Exchange Marauder March 2021)(Citation: Symantec Attacks Against Government Sector) Windows Security Support Provider (SSP) DLLs are loaded into LSASS process at system start. Once loaded into the LSA, SSP DLLs have access to encrypted and plaintext passwords that are stored in Windows, such as any logged-on user's Domain password or smart card PINs. The SSP configuration is stored in two Registry keys: `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages` and `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages`. An adversary may modify these Registry keys to add new SSPs, which will be loaded the next time the system boots, or when the AddSecurityPackage Windows API function is called.(Citation: Graeber 2014) The following SSPs can be used to access credentials: * Msv: Interactive logons, batch logons, and service logons are done through the MSV authentication package. * Wdigest: The Digest Authentication protocol is designed for use with Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) exchanges.(Citation: TechNet Blogs Credential Protection) * Kerberos: Preferred for mutual client-server domain authentication in Windows 2000 and later. * CredSSP: Provides SSO and Network Level Authentication for Remote Desktop Services.(Citation: TechNet Blogs Credential Protection)

Name

T1566

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

T1204

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

T1036

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) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

T1140

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

T1071

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

T1566.001

ID

T1566.001

Description

Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon [User Execution](https://attack.mitre.org/techniques/T1204) to gain execution. Spearphishing may also involve social engineering techniques, such as posing as a trusted source. There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

Name

T1071.004

ID

T1071.004

Description

Adversaries may communicate using the Domain Name System (DNS) application layer protocol 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. The DNS protocol serves an administrative function in computer networking and thus may be very common in environments. DNS traffic may also be allowed even before network authentication is completed. DNS packets contain many fields and headers in which data can be concealed. Often known as DNS tunneling, adversaries may abuse DNS to communicate with systems under their control within a victim network while also mimicking normal, expected traffic. (Citation: PAN DNS Tunneling)(Citation: Medium DnsTunneling)

Name

T1568.002

ID

T1568.002

Description
Adversaries may make use of Domain Generation Algorithms (DGAs) to dynamically identify a destination domain for command and control traffic rather than relying on a list of static IP addresses or domains. This has the advantage of making it much harder for defenders to block, track, or take over the command and control channel, as there potentially could be thousands of domains that malware can check for instructions.(Citation: Cybereason Dissecting DGAs)(Citation: Cisco Umbrella DGA)(Citation: Unit 42 DGA Feb 2019) DGAs can take the form of apparently random or "gibberish" strings (ex: istgmxdejdnxuyla.ru) when they construct domain names by generating each letter. Alternatively, some DGAs employ whole words as the unit by concatenating words together instead of letters (ex: cityjulydish.net). Many DGAs are time-based, generating a different domain for each time period (hourly, daily, monthly, etc). Others incorporate a seed value as well to make predicting future domains more difficult for defenders.(Citation: Cybereason Dissecting DGAs)(Citation: Cisco Umbrella DGA)(Citation: Talos CCleanup 2017)(Citation: Akamai DGA Mitigation) Adversaries may use DGAs for the purpose of [Fallback Channels](https://attack.mitre.org/techniques/T1008). When contact is lost with the primary command and control server malware may employ a DGA as a means to reestablishing command and control.(Citation: Talos CCleanup 2017)(Citation: FireEye POSHSPY April 2017)(Citation: ESET Sednit 2017 Activity)

Name
T1003

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.

Country

Name
Ukraine

Name
BY

Name
Georgia

Name
KZ

Name
United States of America

Name
South Georgia and the South Sandwich Islands

Name
AR

Region

Name
Eastern Europe

Name
Europe

Name
Middle East

Name
Central Asia

Name
Asia

Name
Northern America

Name
Latin America and the Caribbean

Name
Americas

Hostname

Value
sgg-gov.firstcloudit.com
sgg-files.firstcloudit.com
rada-zakon.firstcloudit.com
presidencia-gov.firstcloudit.com
presidencia-gob.firstcloudit.com
presidencia-files.firstcloudit.com
presidencia-docs.firstcloudit.com
militarysupport.firstcloudit.com
kzgw-wody.firstcloudit.com
gcsd.firstcloudit.com
files-presidencia.firstcloudit.com
emod.firstcloudit.com
eecommission.firstcloudit.com

eecommission-drive.firstcloudit.com
e-presidencia.firstcloudit.com
e-military.firstcloudit.com
e-gov.firstcloudit.com
e-gov-am.firstcloudit.com
dls-gov.firstcloudit.com
calendarua.firstcloudit.com
calendar-ua.firstcloudit.com
wody-info-files.firstcloudit.com
webmail.facadesolutionsuae.com
ua-calendar.firstcloudit.com
nas-files.firstcloudit.com
info-mod.firstcloudit.com
e-nas.firstcloudit.com
e-mod.firstcloudit.com

IPv4-Addr

Value
148.252.42.42
194.126.178.8

StixFile

Value
64b0037dde987c78edf807a1bd7f09cdfac072ec2a59954cc4918828b7e608a3
451f3d427ac21632f38619ef96dece25798918866d44fe82ff1ed30996f998dc
40a7fd89b9e51b0a515ac2355036d203357be90a2200b9c506b95c12db54c7aa
18f891a3737bb53cd1ab451e2140654a376a43b2d75f6695f3133d47a41952b6
24fd571600dcc00bf2bb8577c7e4fd67275f7d19d852b909395bebcbb1274e04

External References

- https://securityintelligence.com/x-force/itg05-leverages-malware-arsenal
- https://otx.alienvault.com/pulse/65f422be7fd82b8a6cef5ac9