Sep 25 2023

NETMANAGEIT

Intelligence Report

Examining the Activities of the Turla APT Group

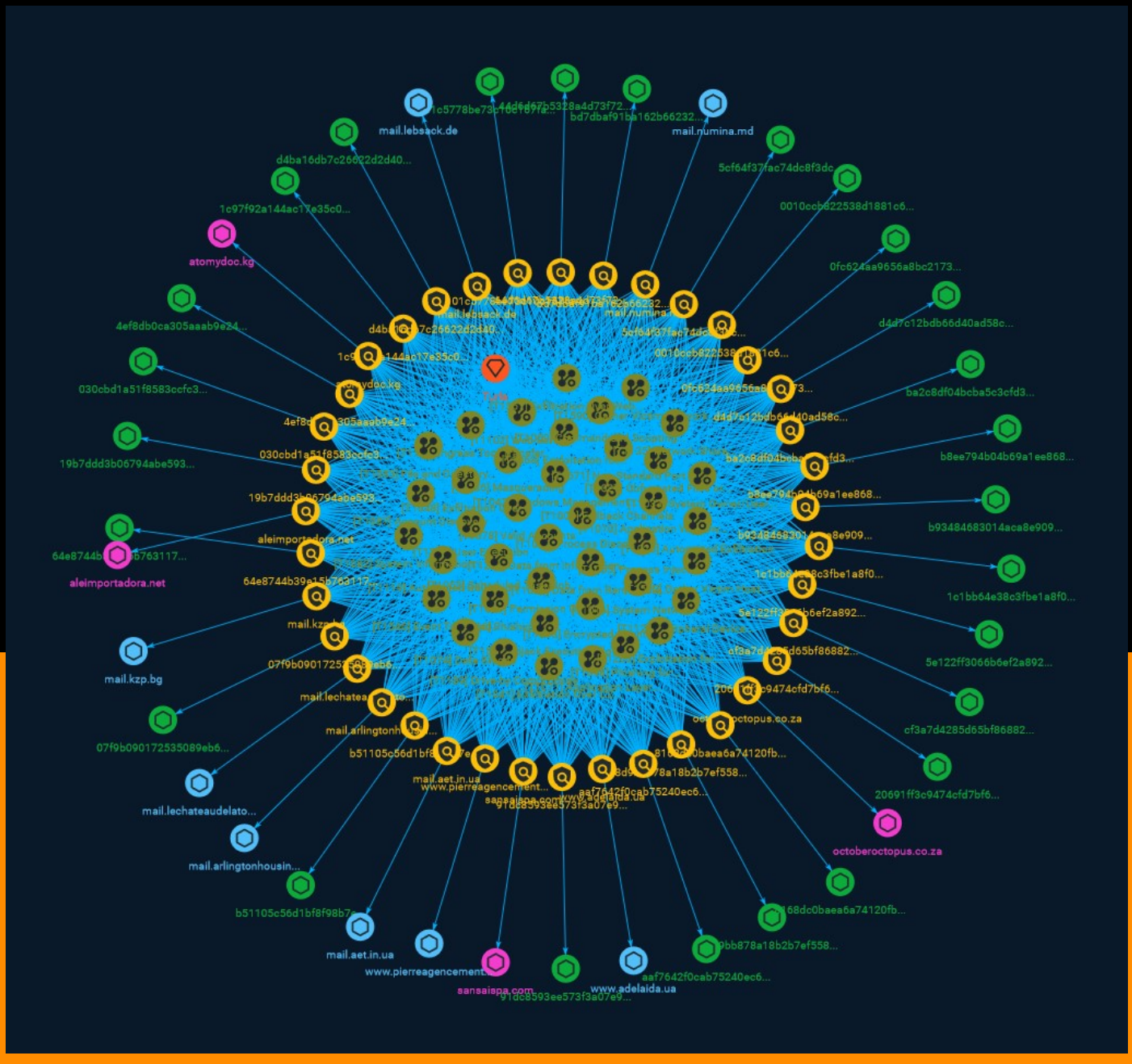

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Turla's group names are infamously titled after its top-class rootkits such as Snake, Venomous Bear, WhiteBear, Uroburos, Group 88, and Waterbug, all known for targeting government entities, intelligence agencies, as well as the military, educational, research, and pharmaceutical industries around the world. Like other APT groups, Turla possesses its own specifically-designed, complex tools. However, it is the threat actor's satellite-based command-and-control (C&C) mechanism that it uses in the latter stages of an attack, coupled with its ability to fly under the radar, that makes Turla stand out from its contemporaries.

Confidence

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

15 / 100

Attack-Pattern

Name

Process Discovery

ID

T1057

Description

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from [Process Discovery](https://attack.mitre.org/techniques/T1057) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. In Windows environments, adversaries could obtain details on running processes using the [Tasklist](https://attack.mitre.org/software/S0057) utility via [cmd](https://attack.mitre.org/software/S0106) or `Get-Process` via [PowerShell](https://attack.mitre.org/techniques/T1059/001). Information about processes can also be extracted from the output of [Native API](https://attack.mitre.org/techniques/T1106) calls such as `CreateToolhelp32Snapshot`. In Mac and Linux, this is accomplished with the `ps` command. Adversaries may also opt to enumerate processes via /proc. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show processes` can be used to display current running processes.(Citation: US-CERT-TA18-106A)(Citation: show_processes_cisco_cmd)

Name

Data from Information Repositories

ID

T1213

Description

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

Name

Windows Management Instrumentation

ID

T1047

Description

Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. WMI is an administration feature that provides a uniform environment to access Windows system components. The WMI service enables both local and remote access, though the latter is facilitated by [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) (DCOM) and [Windows Remote Management]

(https://attack.mitre.org/techniques/T1021/006) (WinRM).(Citation: MSDN WMI) Remote WMI over DCOM operates using port 135, whereas WMI over WinRM operates over port 5985 when using HTTP and 5986 for HTTPS.(Citation: MSDN WMI)(Citation: FireEye WMI 2015) An adversary can use WMI to interact with local and remote systems and use it as a means to execute various behaviors, such as gathering information for Discovery as well as remote Execution of files as part of Lateral Movement. (Citation: FireEye WMI SANS 2015) (Citation: FireEye WMI 2015)

Name

Data from Removable Media

ID

T1025

Description

Adversaries may search connected removable media on computers they have compromised to find files of interest. Sensitive data can be collected from any removable media (optical disk drive, USB memory, etc.) connected to the compromised system prior to Exfiltration. Interactive command shells may be in use, and common functionality within [cmd](https://attack.mitre.org/software/S0106) may be used to gather information. Some adversaries may also use [Automated Collection](https://attack.mitre.org/techniques/T1119) on removable media.

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

Fallback Channels

ID

T1008

Description

Adversaries may use fallback or alternate communication channels if the primary channel is compromised or inaccessible in order to maintain reliable command and control and to avoid data transfer thresholds.

Name

Permission Groups Discovery

ID

T1069

Description

Adversaries may attempt to discover group and permission settings. This information can help adversaries determine which user accounts and groups are available, the membership of users in particular groups, and which users and groups have elevated permissions. Adversaries may attempt to discover group permission settings in many different ways. This data may provide the adversary with information about the compromised environment that can be used in follow-on activity and targeting.(Citation: CrowdStrike BloodHound April 2018)

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

Process Injection

ID

T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

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

Non-Standard Port

ID

T1571

Description

Adversaries may communicate using a protocol and port pairing that are typically not associated. For example, HTTPS over port 8088(Citation: Symantec Elfin Mar 2019) or port 587(Citation: Fortinet Agent Tesla April 2018) as opposed to the traditional port 443. Adversaries may make changes to the standard port used by a protocol to bypass filtering or muddle analysis/parsing of network data. Adversaries may also make changes to victim systems to abuse non-standard ports. For example, Registry keys and other configuration settings can be used to modify protocol and port pairings.(Citation: change_rdp_port_conti)

Name

Encrypted Channel

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

Exfiltration Over Alternative Protocol

ID

T1048

Description

Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server. Alternate protocols include FTP, SMTP, HTTP/S, DNS, SMB, or any other network protocol not being used as the main command and control channel. Adversaries may also opt to encrypt and/or obfuscate these alternate channels. [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048) can be done using various common operating system utilities such as [Net](https://attack.mitre.org/software/S0039)/SMB or FTP.(Citation: Palo Alto OilRig Oct 2016) On macOS and Linux `curl` may be used to invoke protocols such as HTTP/S or FTP/S to exfiltrate data from a system.(Citation: 20 macOS Common Tools and Techniques) Many IaaS and SaaS platforms (such as Microsoft Exchange, Microsoft SharePoint, GitHub, and AWS S3) support the direct download of files, emails, source code, and other sensitive information via the web console or [Cloud API](https://attack.mitre.org/techniques/T1059/009).

Name

Application Window Discovery

ID

T1010

Description

Adversaries may attempt to get a listing of open application windows. Window listings could convey information about how the system is used.(Citation: Prevailion DarkWatchman 2021) For example, information about application windows could be used identify potential data to collect as well as identifying security tooling ([Security Software Discovery](https://attack.mitre.org/techniques/T1518/001)) to evade.(Citation: ESET Grandoreiro April 2020) Adversaries typically abuse system features for this type of enumeration. For example, they may gather information through native system features such as [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) commands and [Native API](https://attack.mitre.org/techniques/T1106) functions.

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

Exploitation for Privilege Escalation

ID

T1068

Description

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions. When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods. Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020) Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a compromised system via [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) or [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570).

Name

System Network Configuration Discovery

ID

T1016

Description

Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include [Arp](https://attack.mitre.org/software/S0099),

[ipconfig](https://attack.mitre.org/software/S0100)/[ifconfig](https://attack.mitre.org/software/S0101), [nbtstat](https://attack.mitre.org/software/S0102), and [route](https://attack.mitre.org/software/S0103). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather information about configurations and settings, such as IP addresses of configured interfaces and static/dynamic routes (e.g. `show ip route`, `show ip interface`).(Citation: US-CERT-TA18-106A)(Citation: Mandiant APT41 Global Intrusion) Adversaries may use the information from [System Network Configuration Discovery](https://attack.mitre.org/techniques/T1016) during automated discovery to shape follow-on behaviors, including determining certain access within the target network and what actions to do next.

Name

User Execution

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

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

Ingress Tool Transfer

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`. (Citation: t1105_lolbas)

Name

Gather Victim Host Information

ID

T1592

Description

Adversaries may gather information about the victim's hosts that can be used during targeting. Information about hosts may include a variety of details, including administrative data (ex: name, assigned IP, functionality, etc.) as well as specifics regarding its configuration (ex: operating system, language, etc.). 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). Adversaries may also compromise sites then include malicious content designed to collect host information from visitors.(Citation: ATT ScanBox) Information about hosts may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195) or [External Remote Services](https://attack.mitre.org/techniques/T1133)).

Name

Event Triggered Execution

ID

T1546

Description

Adversaries may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events. Various operating systems have means to monitor and subscribe to events such as logons or other user activity such as running specific applications/binaries. Cloud environments may also support various functions and services that monitor and can be invoked in response to specific cloud events. (Citation: Backdooring an AWS account)(Citation: Varonis Power Automate Data Exfiltration) (Citation: Microsoft DART Case Report 001) Adversaries may abuse these mechanisms as a means of maintaining persistent access to a victim via repeatedly executing malicious code. After gaining access to a victim system, adversaries may create/modify event triggers to point to malicious content that will be executed whenever the event trigger is invoked. (Citation: FireEye WMI 2015)(Citation: Malware Persistence on OS X)(Citation: amnesia malware) Since the execution can be proxied by an account with higher permissions, such as SYSTEM or service accounts, an adversary may be able to abuse these triggered execution mechanisms to escalate their privileges.

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

Phishing for Information

ID

T1598

Description

Adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Phishing for information is different from [Phishing](https://attack.mitre.org/techniques/T1566) in that the objective is gathering data from the victim rather than executing malicious code. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass credential harvesting campaigns. Adversaries may also try to obtain information directly through the exchange of emails, instant messages, or other electronic conversation means.(Citation: ThreatPost Social Media Phishing)(Citation: TrendMictro Phishing)(Citation: PCMag FakeLogin)(Citation: Sophos Attachment)(Citation: GitHub Phishery) Victims may also receive phishing messages that direct them to call a phone number where the adversary attempts to collect confidential information.(Citation: Avertium callback phishing) Phishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)) and/or sending multiple, seemingly urgent messages. Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Phishing for information may also involve evasive techniques, such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)). (Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014)

Name

Account Discovery

ID

T1087

Description

Adversaries may attempt to get a listing of valid accounts, usernames, or email addresses on a system or within a compromised environment. This information can help adversaries determine which accounts exist, which can aid in follow-on behavior such as brute-forcing, spear-phishing attacks, or account takeovers (e.g., [Valid Accounts](https://attack.mitre.org/techniques/T1078)). Adversaries may use several methods to enumerate accounts, including abuse of existing tools, built-in commands, and potential misconfigurations that leak account names and roles or permissions in the targeted environment. For examples, cloud environments typically provide easily accessible interfaces to obtain user lists. On hosts, adversaries can use default [PowerShell](https://attack.mitre.org/techniques/T1059/001) and other command line functionality to identify accounts. Information about email addresses and accounts may also be extracted by searching an infected system's files.

Name

System Owner/User Discovery

ID

T1033

Description

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). The information may be collected in a number of different ways using other Discovery techniques, because user and username details are

prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from [System Owner/User Discovery](https://attack.mitre.org/techniques/T1033) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Various utilities and commands may acquire this information, including `whoami`. In macOS and Linux, the currently logged in user can be identified with `w` and `who`. On macOS the `dscl . list /Users | grep -v '_'` command can also be used to enumerate user accounts. Environment variables, such as `%USERNAME%` and `$USER`, may also be used to access this information. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show users` and `show ssh` can be used to display users currently logged into the device.(Citation: show_ssh_users_cmd_cisco)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)

Name

Drive-by Compromise

ID

T1189

Description

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring [Application Access Token](https://attack.mitre.org/techniques/T1550/001). Multiple ways of delivering exploit code to a browser exist (i.e., [Drive-by Target](https://attack.mitre.org/techniques/T1608/004)), including: * A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting * Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary * Malicious ads are paid for and served through legitimate ad providers (i.e., [Malvertising](https://attack.mitre.org/techniques/T1583/008)) * Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content). Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering

hole attack. There are several known examples of this occurring.(Citation: Shadowserver Strategic Web Compromise) Typical drive-by compromise process: 1. A user visits a website that is used to host the adversary controlled content. 2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version. * The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes. 3. Upon finding a vulnerable version, exploit code is delivered to the browser. 4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place. * In some cases a second visit to the website after the initial scan is required before exploit code is delivered. Unlike [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ. Adversaries may also use compromised websites to deliver a user to a malicious application designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.(Citation: Volexity OceanLotus Nov 2017)

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

Peripheral Device Discovery

ID

T1120

Description

Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system.(Citation: Peripheral Discovery Linux) (Citation: Peripheral Discovery macOS) Peripheral devices could include auxiliary resources that support a variety of functionalities such as keyboards, printers, cameras, smart card readers, or removable storage. The information may be used to enhance their awareness of the system and network environment or may be used for further actions.

Name

Automated Collection

ID

T1119

Description

Once established within a system or network, an adversary may use automated techniques for collecting internal data. Methods for performing this technique could include use of a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) to search for and copy information fitting set criteria such as file type, location, or name at specific time intervals. In cloud-based environments, adversaries may also use cloud APIs, command line interfaces, or extract, transform, and load (ETL) services to automatically collect data. This functionality could also be built into remote access tools. This technique may incorporate use of other techniques such as [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) and [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570) to identify and move files, as well as [Cloud Service Dashboard](https://

attack.mitre.org/techniques/T1538) and [Cloud Storage Object Discovery](https://attack.mitre.org/techniques/T1619) to identify resources in cloud environments.

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

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

File and Directory Discovery

ID

T1083

Description

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include `dir`, `tree`, `ls`, `find`, and `locate`.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information (e.g. `dir`, `show flash`, and/or `nvram`).(Citation: US-CERT-TA18-106A)

Name

Automated Exfiltration

ID

T1020

Description

Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection. When automated exfiltration is used, other exfiltration techniques likely apply as well to transfer the information out of the network, such as [Exfiltration Over C2 Channel](https://attack.mitre.org/techniques/T1041) and [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048).

Name

Data Staged

ID

T1074

Description

Adversaries may stage collected data in a central location or directory prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as [Archive Collected Data](https://attack.mitre.org/techniques/T1560). Interactive command shells may be used, and common functionality within [cmd](https://attack.mitre.org/software/S0106) and bash may be used to copy data into a staging location.(Citation: PWC Cloud Hopper April 2017) In cloud environments, adversaries may stage data within a particular instance or virtual machine before exfiltration. An adversary may [Create Cloud Instance](https://attack.mitre.org/techniques/T1578/002) and stage data in that instance.(Citation: Mandiant M-Trends 2020) Adversaries may choose to stage data from a victim network in a centralized location prior to Exfiltration to minimize the number of connections made to their C2 server and better evade detection.

Name

Exfiltration Over Web Service

ID

T1567

Description

Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel. Popular Web services acting as an exfiltration mechanism may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to compromise. Firewall rules may also already exist to permit traffic to these services. Web service providers also commonly use SSL/TLS encryption, giving adversaries an added level of protection.

Name

Exploitation for Client Execution

ID

T1203

Description

Adversaries may exploit software vulnerabilities in client applications to execute code. Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behavior. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Oftentimes the most valuable exploits to an offensive toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to do work, so they are a useful target for exploit research and development because of their high utility. Several types exist: ### Browser-based Exploitation Web browsers are a common target through [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) and [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002). Endpoint systems may be compromised through normal web browsing or from certain users being targeted by links in spearphishing emails to adversary controlled sites used to exploit the web browser. These often do not require an action by the user for the exploit to be executed. ### Office Applications Common office and productivity applications such as Microsoft Office are also targeted through [Phishing](https://attack.mitre.org/techniques/T1566). Malicious files will be transmitted directly as attachments or through links to download

them. These require the user to open the document or file for the exploit to run. ### Common Third-party Applications Other applications that are commonly seen or are part of the software deployed in a target network may also be used for exploitation. Applications such as Adobe Reader and Flash, which are common in enterprise environments, have been routinely targeted by adversaries attempting to gain access to systems. Depending on the software and nature of the vulnerability, some may be exploited in the browser or require the user to open a file. For instance, some Flash exploits have been delivered as objects within Microsoft Office documents.

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)

Name

Network Share Discovery

ID

T1135

Description

Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement. Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network. File sharing over a Windows network occurs over the SMB protocol. (Citation: Wikipedia Shared Resource) (Citation: TechNet Shared Folder) [Net](https://attack.mitre.org/software/S0039) can be used to query a remote system for available shared drives using the `net view \\\\remotesystem` command. It can also be used to query shared drives on the local system using `net share`. For macOS, the `sharing -l` command lists all shared points used for smb services.

Name

Exfiltration Over C2 Channel

ID

T1041

Description

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Indicator

Name
4ef8db0ca305aaab9e2471b198168021c531862cb4319098302026b1cfa89947
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '4ef8db0ca305aaab9e2471b198168021c531862cb4319098302026b1cfa89947']
Name
b93484683014aca8e909c9b5648d8f0ac21a45d0c193f6ca40f0b01d2464c1c4
Description
Win.Trojan.ComRAT-9797302-0 SHA256 of d117643019d665a29ce8a7b812268fb8d3e5aadb
Pattern Type
stix
Pattern

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

Name

b51105c56d1bf8f98b7e924aa5caded8322d037745a128781fa0bc23841d1e70

Description

SHA256 of c30af6fa5df14e1ba9355b60a9214937f6f18990

Pattern Type

stix

Pattern

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

Name

44d6d67b5328a4d73f72d8a0f9d39fe4bb6539609f90f169483936a8b3b88316

Description

stack_string SHA256 of ca16a95cd38707bad2dc524bb3086b3c0cb3e372

Pattern Type

stix

Pattern

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

Name

octoberoctopus.co.za

Pattern Type

stix

Pattern

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

Name

64e8744b39e15b76311733014327311acd77330f8a135132f020eac78199ac8a

Description

DotNET_SmartAssembly

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '64e8744b39e15b76311733014327311acd77330f8a135132f020eac78199ac8a']

Name

0fc624aa9656a8bc21731bfc47fd7780da38a7e8ad7baf1529ccd70a5bb07852

Description

ALFPER:Trojan:MSIL/Kapooshka.B!dha SHA256 of 902b27a5fd2e5f17e5340e350afa037549ce9faa

Pattern Type

stix

Pattern

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

Name

91dc8593ee573f3a07e9356e65e06aed58d8e74258313e3414a7de278b3b5233

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '91dc8593ee573f3a07e9356e65e06aed58d8e74258313e3414a7de278b3b5233']

Name

1c97f92a144ac17e35c0e40dc89e12211ef5a7d5eb8db57ab093987ae6f3b9dc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1c97f92a144ac17e35c0e40dc89e12211ef5a7d5eb8db57ab093987ae6f3b9dc']

Name

5e122ff3066b6ef2a89295df925431c151f1713708c99772687a30c3204064bd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5e122ff3066b6ef2a89295df925431c151f1713708c99772687a30c3204064bd']

Name

mail.lechateaudelatour.fr

Pattern Type

stix

Pattern

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

Name

mail.numina.md

Pattern Type

stix

Pattern

[hostname:value = 'mail.numina.md']

Name

8d9bb878a18b2b7ef558504e78a59eb644f83a63679658533ff8accf0b85fda3

Description

Recon_Commands_Windows_Gen1 SHA256 of b627963a9bac33fa6e3de0f9469b2fa5ecdef6ae

Pattern Type

stix

Pattern

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

Name

19b7ddd3b06794abe593bf533d88319711ca15bb0a08901b4ab7e52aab015452

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '19b7ddd3b06794abe593bf533d88319711ca15bb0a08901b4ab7e52aab015452']

Name
ba2c8df04bcba5c3cfd343a59d8b59b76779e6c27eb27b7ac73ded97e08f0f39
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'ba2c8df04bcba5c3cfd343a59d8b59b76779e6c27eb27b7ac73ded97e08f0f39']
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

20691ff3c9474cfd7bf6fa3f8720eb7326e6f87f64a1f190861589c1e7397fa5

Description

SHA256 of 36bba4d26ecf02623a51c6241133c4290551e27f

Pattern Type

stix

Pattern

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

Name

mail.kzp.bg

Pattern Type

stix

Pattern

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

Name

0010ccb822538d1881c61be874af49382c44b6c9cb665081cf0f672cbed5b6a5

Description

vad_contains_network_strings SHA256 of a4aff23b9a58b598524a71f09aa67994083a9c83

Pattern Type

stix

Pattern

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

Name

www.adelaida.ua

Pattern Type

stix

Pattern

[hostname:value = 'www.adelaida.ua']

Name

atomydoc.kg

Pattern Type

stix

Pattern

[domain-name:value = 'atomydoc.kg']

Name

1c1bb64e38c3fbe1a8f0dcb94ded96b332296bcbf839de438a4838fb43b20af3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1c1bb64e38c3fbe1a8f0dcb94ded96b332296bcbf839de438a4838fb43b20af3']

Name

mail.arlingtonhousing.us

Pattern Type

stix

Pattern

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

Name

bd7dbaf91ba162b6623292ebcdd2768c5d87e518240fe8ca200a81e9c7f01d76

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bd7dbaf91ba162b6623292ebcdd2768c5d87e518240fe8ca200a81e9c7f01d76']

Name

8168dc0baea6a74120fbabea261e83377697cb5f9726a2514f38ed04b46c56c8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8168dc0baea6a74120fbabea261e83377697cb5f9726a2514f38ed04b46c56c8']

Name

aleimportadora.net

Pattern Type

stix

Pattern

[domain-name:value = 'aleimportadora.net']

Name

d4d7c12bdb66d40ad58c211dc6dd53a7494e03f9883336fa5464f0947530709f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd4d7c12bdb66d40ad58c211dc6dd53a7494e03f9883336fa5464f0947530709f']

Name

sansaispa.com

Pattern Type

stix

Pattern

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

Name

d4ba16db7c26622d2d402cb9714331abfee891b6276d16e6c2f2132e8944cc71

Description

ALFPER:Trojan:Win32/RoubmaniPot.A!dha SHA256 of 6239b4d374539c940cffa698e0993d199918a2fc

Pattern Type

stix

Pattern

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

Name

cf3a7d4285d65bf8688215407bce1b51d7c6b22497f09021f0fce31cbeb78986

Description

SHA256 of 7c1b25518dee1e30b5a6eaa1ea8e4a3780c24d0c

Pattern Type

stix

Pattern

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

Name

07f9b090172535089eb62a175e5deaf95853fdfd4bcabf099619c60057d38c57

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '07f9b090172535089eb62a175e5deaf95853fdfd4bcabf099619c60057d38c57']

Name

5cf64f37fac74dc8f3dcb58831c3f2ce2b3cf522db448b40acdab254dd46cb3e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5cf64f37fac74dc8f3dcb58831c3f2ce2b3cf522db448b40acdab254dd46cb3e']

Name

aaf7642f0cab75240ec65bc052a0a602366740b31754156b3a0c44dccec9bebe

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'aaf7642f0cab75240ec65bc052a0a602366740b31754156b3a0c44dccec9bebe']

Name

030cbd1a51f8583ccfc3fa38a28a5550dc1c84c05d6c0f5eb887d13dedf1da01

Pattern Type

stix

Pattern

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

Name

b8ee794b04b69a1ee8687daabfe4f912368a500610a099e3072b03eeb66077f8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b8ee794b04b69a1ee8687daabfe4f912368a500610a099e3072b03eeb66077f8']

Name

mail.aet.in.ua

Pattern Type

stix

Pattern

[hostname:value = 'mail.aet.in.ua']

Name

01c5778be73c10c167fae6d7970c0be23a29af1873d743419b1803c035d92ef7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '01c5778be73c10c167fae6d7970c0be23a29af1873d743419b1803c035d92ef7']

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)

Domain-Name

Value
aleimportadora.net
sansaispa.com
atomydoc.kg
octoberoctopus.co.za

StixFile

Value
8d9bb878a18b2b7ef558504e78a59eb644f83a63679658533ff8accf0b85fda3
030cbd1a51f8583ccfc3fa38a28a5550dc1c84c05d6c0f5eb887d13dedf1da01
5cf64f37fac74dc8f3dcb58831c3f2ce2b3cf522db448b40acdab254dd46cb3e
01c5778be73c10c167fae6d7970c0be23a29af1873d743419b1803c035d92ef7
bd7dbaf91ba162b6623292ebcdd2768c5d87e518240fe8ca200a81e9c7f01d76
91dc8593ee573f3a07e9356e65e06aed58d8e74258313e3414a7de278b3b5233
b51105c56d1bf8f98b7e924aa5caded8322d037745a128781fa0bc23841d1e70
b8ee794b04b69a1ee8687daabfe4f912368a500610a099e3072b03eeb66077f8
44d6d67b5328a4d73f72d8a0f9d39fe4bb6539609f90f169483936a8b3b88316
1c97f92a144ac17e35c0e40dc89e12211ef5a7d5eb8db57ab093987ae6f3b9dc
b93484683014aca8e909c9b5648d8f0ac21a45d0c193f6ca40f0b01d2464c1c4
d4ba16db7c26622d2d402cb9714331abfee891b6276d16e6c2f2132e8944cc71
0fc624aa9656a8bc21731bfc47fd7780da38a7e8ad7baf1529ccd70a5bb07852

aaf7642f0cab75240ec65bc052a0a602366740b31754156b3a0c44dccec9bebe

5e122ff3066b6ef2a89295df925431c151f1713708c99772687a30c3204064bd

1c1bb64e38c3fbe1a8f0dcb94ded96b332296bcbf839de438a4838fb43b20af3

d4d7c12bdb66d40ad58c211dc6dd53a7494e03f9883336fa5464f0947530709f

07f9b090172535089eb62a175e5deaf95853fdfd4bcabf099619c60057d38c57

64e8744b39e15b76311733014327311acd77330f8a135132f020eac78199ac8a

4ef8db0ca305aaab9e2471b198168021c531862cb4319098302026b1cfa89947

19b7ddd3b06794abe593bf533d88319711ca15bb0a08901b4ab7e52aab015452

8168dc0baea6a74120fbabea261e83377697cb5f9726a2514f38ed04b46c56c8

20691ff3c9474cfd7bf6fa3f8720eb7326e6f87f64a1f190861589c1e7397fa5

cf3a7d4285d65bf8688215407bce1b51d7c6b22497f09021f0fce31cbeb78986

0010ccb822538d1881c61be874af49382c44b6c9cb665081cf0f672cbed5b6a5

ba2c8df04bcba5c3cfd343a59d8b59b76779e6c27eb27b7ac73ded97e08f0f39

Hostname

Value
www.pierreagencement.fr
mail.aet.in.ua
mail.numina.md
mail.arlingtonhousing.us
mail.lebsack.de
mail.lechateaudelatour.fr
www.adelaida.ua
mail.kzp.bg

External References

- https://otx.alienvault.com/pulse/6511f2ed6d40e649fa850950
- https://www.trendmicro.com/content/dam/trendmicro/global/en/research/23/i/examining-the-activities-of-the-turla-apt-group/ioc-examining-the-activities-of-the-turla-apt-group.txt
- https://www.trendmicro.com/en_us/research/23/i/examining-the-activities-of-the-turla-group.html