May 10 2024

NETMANAGEIT

Intelligence Report

Malware (XMRig, OrcusRAT, etc.) disguised as MS Office crack

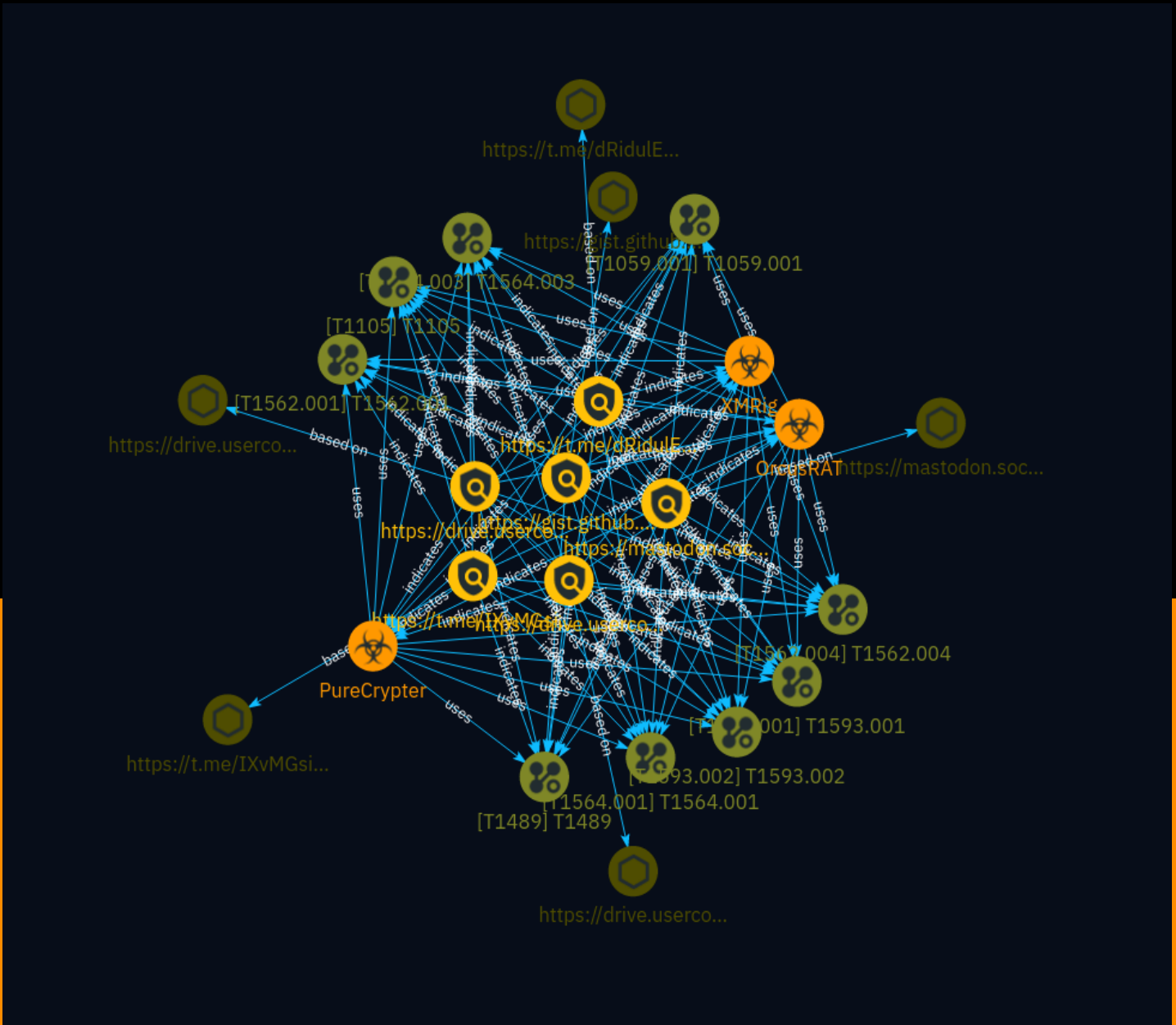

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The report details an ongoing malware campaign targeting South Korean users, which disguises malicious payloads as cracked versions of Microsoft Office and other popular software. The attackers are distributing a variety of malware, including downloaders, coin miners, remote access tools (RATs), proxies, and anti-antivirus components. These are installed persistently through scheduled tasks and utilise encoded PowerShell commands for updates. The primary malware families identified include Orcus RAT for system control, XMRig cryptominer, 3Proxy for creating a proxy network, and components to evade security products.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
https://gist.github.com/thamanarya/6510d9e6b96adfea6b9422a3fd22ef82/raw/Power
Pattern Type
stix
Pattern
[url:value = 'https://gist.github.com/thamanarya/6510d9e6b96adfea6b9422a3fd22ef82/raw/Power']
Name
https://drive.usercontent.google.com/download?id=1SFoSCa4PhCsR7ACj8HUIfrU7L1i8YwiR&export=download
Pattern Type
stix
Pattern
[url:value = 'https://drive.usercontent.google.com/download?id=1SFoSCa4PhCsR7ACj8HUIfrU7L1i8YwiR&export=download']

Name

https://drive.usercontent.google.com/download?id=1kFPqJkzWKIIQzC3b0b6nunctXKHPeJNi&export=download

Pattern Type

stix

Pattern

[url:value = 'https://drive.usercontent.google.com/download?id=1kFPqJkzWKIIQzC3b0b6nunctXKHPeJNi&export=download']

Name

https://mastodon.social/@dRidulEDhRQYNREkN

Pattern Type

stix

Pattern

[url:value = 'https://mastodon.social/@dRidulEDhRQYNREkN']

Name

https://t.me/IXvMGsiyPuHoPSSiD

Pattern Type

stix

Pattern

[url:value = 'https://t.me/IXvMGsiyPuHoPSSiD']

Name

https://t.me/dRidulEDhRQYNREkN

Pattern Type

stix

Pattern

[url:value = 'https://t.me/dRidulEDhRQYNREkN']

Malware

Name
OrcusRAT

Name
PureCrypter

Name
XMRig

Attack-Pattern

Name
T1564.001
ID
T1564.001
Description
Adversaries may set files and directories to be hidden to evade detection mechanisms. To prevent normal users from accidentally changing special files on a system, most operating systems have the concept of a ‘hidden’ file. These files don’t show up when a user browses the file system with a GUI or when using normal commands on the command line. Users must explicitly ask to show the hidden files either via a series of Graphical User Interface (GUI) prompts or with command line switches (`dir /a` for Windows and `ls –a` for Linux and macOS). On Linux and Mac, users can mark specific files as hidden simply by putting a “.” as the first character in the file or folder name (Citation: Sofacy Komplex Trojan) (Citation: Antiquated Mac Malware). Files and folders that start with a period, ‘.’, are by default hidden from being viewed in the Finder application and standard command-line utilities like “ls”. Users must specifically change settings to have these files viewable. Files on macOS can also be marked with the UF_HIDDEN flag which prevents them from being seen in Finder.app, but still allows them to be seen in Terminal.app (Citation: WireLurker). On Windows, users can mark specific files as hidden by using the attrib.exe binary. Many applications create these hidden files and folders to store information so that it doesn’t clutter up the user’s workspace. For example, SSH utilities create a .ssh folder that’s hidden and contains the user’s known hosts and keys. Adversaries can use this to their advantage to hide files and folders anywhere on the system and evading a typical user or system analysis that does not incorporate investigation of hidden files.

Name

T1564.003

ID

T1564.003

Description

Adversaries may use hidden windows to conceal malicious activity from the plain sight of users. In some cases, windows that would typically be displayed when an application carries out an operation can be hidden. This may be utilized by system administrators to avoid disrupting user work environments when carrying out administrative tasks. Adversaries may abuse these functionalities to hide otherwise visible windows from users so as not to alert the user to adversary activity on the system.(Citation: Antiquated Mac Malware) On macOS, the configurations for how applications run are listed in property list (plist) files. One of the tags in these files can be `apple.awt.UIElement`, which allows for Java applications to prevent the application's icon from appearing in the Dock. A common use for this is when applications run in the system tray, but don't also want to show up in the Dock. Similarly, on Windows there are a variety of features in scripting languages, such as [PowerShell](https://attack.mitre.org/techniques/T1059/001), Jscript, and [Visual Basic](https://attack.mitre.org/techniques/T1059/005) to make windows hidden. One example of this is `powershell.exe -WindowStyle Hidden`.(Citation: PowerShell About 2019) In addition, Windows supports the `CreateDesktop()` API that can create a hidden desktop window with its own corresponding `explorer.exe` process.(Citation: Hidden VNC)(Citation: Anatomy of an hVNC Attack) All applications running on the hidden desktop window, such as a hidden VNC (hVNC) session,(Citation: Hidden VNC) will be invisible to other desktops windows.

Name

T1593.001

ID

T1593.001

Description

Adversaries may search social media for information about victims that can be used during targeting. Social media sites may contain various information about a victim organization, such as business announcements as well as information about the roles, locations, and interests of staff. Adversaries may search in different social media sites depending on what information they seek to gather. Threat actors may passively harvest data from these sites, as well as use information gathered to create fake profiles/groups to elicit victim's into revealing specific information (i.e. [Spearphishing Service](https://attack.mitre.org/techniques/T1598/001)).(Citation: Cyware Social Media) Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Spearphishing via Service](https://attack.mitre.org/techniques/T1566/003)).

Name

T1562.001

ID

T1562.001

Description

Adversaries may modify and/or disable security tools to avoid possible detection of their malware/tools and activities. This may take many forms, such as killing security software processes or services, modifying / deleting Registry keys or configuration files so that tools do not operate properly, or other methods to interfere with security tools scanning or reporting information. Adversaries may also disable updates to prevent the latest security patches from reaching tools on victim systems.(Citation: SCADAfence_ransomware) Adversaries may also tamper with artifacts deployed and utilized by security tools. Security tools may make dynamic changes to system components in order to maintain visibility into specific events. For example, security products may load their own modules and/or modify those loaded by processes to facilitate data collection. Similar to [Indicator Blocking](https://attack.mitre.org/techniques/T1562/006), adversaries may unhook or otherwise modify these features added by tools (especially those that exist in userland or are otherwise potentially accessible to adversaries) to avoid detection.(Citation: OutFlank System Calls)(Citation: MDSec System Calls) Adversaries may also focus on specific applications such as Sysmon. For example, the "Start" and "Enable" values in

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EventLog-Microsoft-Windows-Sysmon-Operational` may be modified to tamper with and potentially disable Sysmon logging.(Citation: disable_win_evt_logging) On network devices, adversaries may attempt to skip digital signature verification checks by altering startup configuration files and effectively disabling firmware verification that typically occurs at boot.(Citation: Fortinet Zero-Day and Custom Malware Used by Suspected Chinese Actor in Espionage Operation)(Citation: Analysis of FG-IR-22-369) In cloud environments, tools disabled by adversaries may include cloud monitoring agents that report back to services such as AWS CloudWatch or Google Cloud Monitor. Furthermore, although defensive tools may have anti-tampering mechanisms, adversaries may abuse tools such as legitimate rootkit removal kits to impair and/or disable these tools.(Citation: chasing_avaddon_ransomware)(Citation: dharma_ransomware)(Citation: demystifying_ryuk)(Citation: doppelpaymer_crowdstrike) For example, adversaries have used tools such as GMER to find and shut down hidden processes and antivirus software on infected systems.(Citation: demystifying_ryuk) Additionally, adversaries may exploit legitimate drivers from anti-virus software to gain access to kernel space (i.e. [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068)), which may lead to bypassing anti-tampering features.(Citation: avoslocker_ransomware)

Name

T1059.001

ID

T1059.001

Description

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems). PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk. A number of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack)

PowerShell commands/scripts can also be executed without directly invoking the `powershell.exe` binary through interfaces to PowerShell's underlying `System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)

Name

T1593.002

ID

T1593.002

Description

Adversaries may use search engines to collect information about victims that can be used during targeting. Search engine services typical crawl online sites to index context and may provide users with specialized syntax to search for specific keywords or specific types of content (i.e. filetypes).(Citation: SecurityTrails Google Hacking)(Citation: ExploitDB GoogleHacking) Adversaries may craft various search engine queries depending on what information they seek to gather. Threat actors may use search engines to harvest general information about victims, as well as use specialized queries to look for spillages/leaks of sensitive information such as network details or credentials. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Valid Accounts](https://attack.mitre.org/techniques/T1078) or [Phishing](https://attack.mitre.org/techniques/T1566)).

Name

T1105

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)). 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) Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. Adversaries have also abused file application features, such as the Windows `search-ms` protocol handler, to deliver malicious files to victims through remote file searches invoked by [User Execution](https://attack.mitre.org/techniques/T1204) (typically after interacting with [Phishing](https://attack.mitre.org/techniques/T1566) lures).(Citation: T1105: Trellix_search-ms) 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) In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.(Citation: Dropbox Malware Sync)

Name

T1562.004

ID

T1562.004

Description

Adversaries may disable or modify system firewalls in order to bypass controls limiting network usage. Changes could be disabling the entire mechanism as well as adding, deleting, or modifying particular rules. This can be done numerous ways depending on the operating system, including via command-line, editing Windows Registry keys, and Windows Control Panel. Modifying or disabling a system firewall may enable adversary C2 communications, lateral movement, and/or data exfiltration that would otherwise not be allowed. For example, adversaries may add a new firewall rule for a well-known protocol (such as RDP) using a non-traditional and potentially less securitized port (i.e. [Non-Standard Port](https://attack.mitre.org/techniques/T1571)).(Citation: change_rdp_port_conti) Adversaries may also modify host networking settings that indirectly manipulate system firewalls, such as interface bandwidth or network connection request thresholds.(Citation: Huntress BlackCat) Settings related to enabling abuse of various [Remote Services](https://attack.mitre.org/techniques/T1021) may also indirectly modify firewall rules.

Name

T1489

ID

T1489

Description

Adversaries may stop or disable services on a system to render those services unavailable to legitimate users. Stopping critical services or processes can inhibit or stop response to an incident or aid in the adversary's overall objectives to cause damage to the environment.(Citation: Talos Olympic Destroyer 2018)(Citation: Novetta Blockbuster) Adversaries may accomplish this by disabling individual services of high importance to an organization, such as `MSExchangeIS`, which will make Exchange content inaccessible (Citation: Novetta Blockbuster). In some cases, adversaries may stop or disable many or all services to render systems unusable.(Citation: Talos Olympic Destroyer 2018) Services or processes may not allow for modification of their data stores while running. Adversaries may stop services or processes in order to conduct [Data Destruction](https://attack.mitre.org/techniques/T1485) or [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486) on the data stores of services like Exchange and SQL Server.(Citation: SecureWorks WannaCry Analysis)

Url

Value
https://gist.github.com/thamanarya/6510d9e6b96adfea6b9422a3fd22ef82/raw/Power
https://drive.usercontent.google.com/download?id=1SFoSCa4PhCsR7ACj8HUIfrU7L1i8YwiR&export=download
https://drive.usercontent.google.com/download?id=1kFPqJkzWKIIQzC3b0b6nunctXKHPeJNi&export=download
https://mastodon.social/@dRidulEDhRQYNREkN
https://t.me/IXvMGsiyPuHoPSSiD
https://t.me/dRidulEDhRQYNREkN

External References

- https://asec.ahnlab.com/ko/65307/
- https://otx.alienvault.com/pulse/663e2509ff80d7938107143b