Apr 08 2024

NETMANAGEIT

Intelligence Report

Raspberry Robin and its new anti-emulation trick

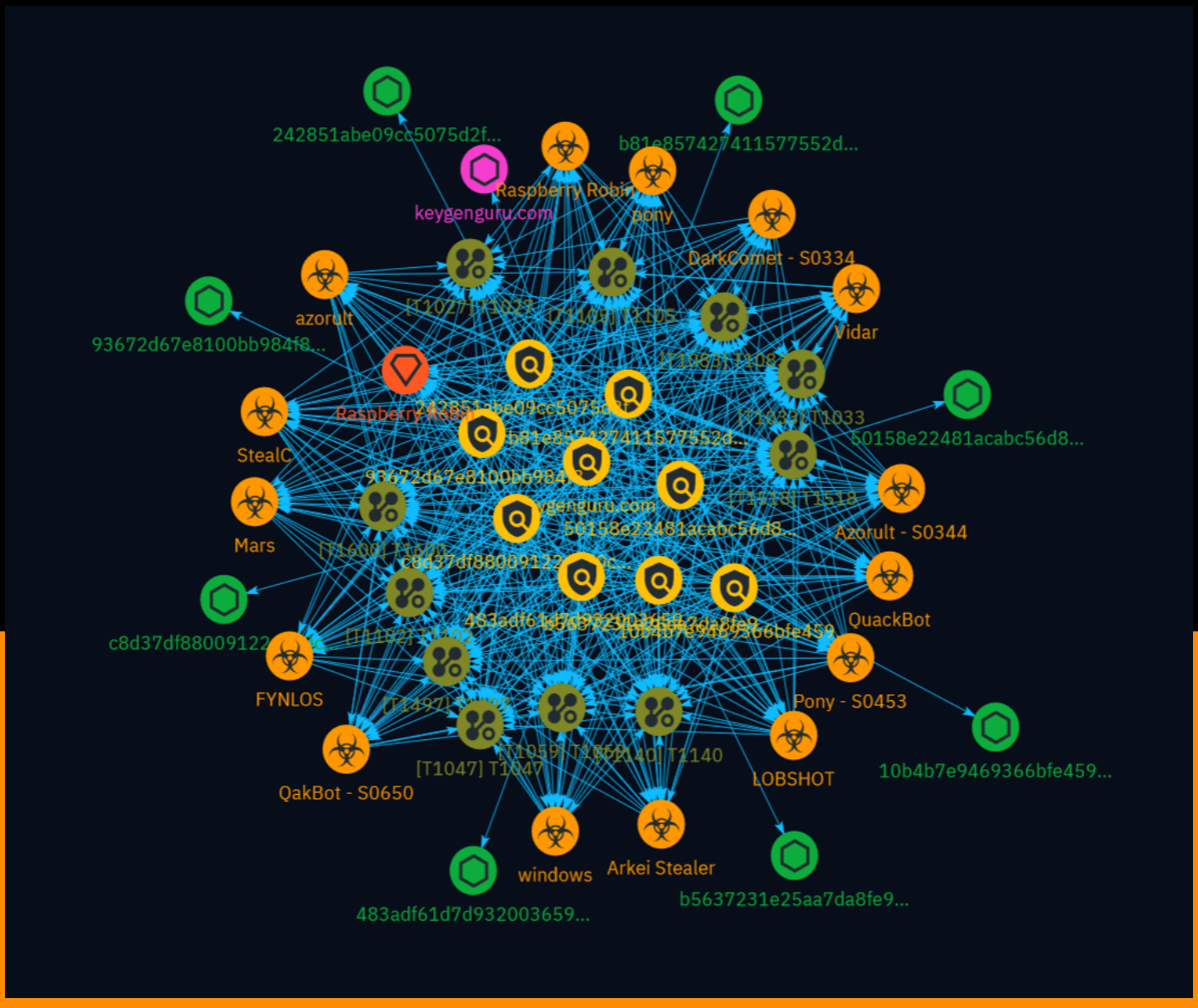

Table of contents

Overview

Entities

Observables

External References

Overview

Description

An analysis of the constantly evolving evasion capabilities employed by the Raspberry Robin malware, which has emerged as a prominent threat. The report delves into the recent variant's unique anti-emulation techniques that leverage undocumented functions from the Windows Defender emulator's virtual DLLs, potentially marking the first instance of such exploitation. It highlights the malware's ability to evade detection and facilitate access for other threat actors, emphasizing the need for proactive countermeasures.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

keygenguru.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 595230 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** Warez - **Domain Age:** {'human': '18 years ago', 'timestamp': 1156349681, 'iso': '2006-08-23T12:14:41-04:00'} - **IPQS: Domain:** keygenguru.com - **IPQS: IP Address:** 104.21.12.55

Pattern Type

stix

Pattern

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

Name

c8d37df88009122c890cb95dc79d895d39339fe1efdcfa5e033d0aea171ffc3d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c8d37df88009122c890cb95dc79d895d39339fe1efdcfa5e033d0aea171ffc3d']

Name

b81e857427411577552d1ecdd444efaeab23ec903192812d40ab3dd69df98ec5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b81e857427411577552d1ecdd444efaeab23ec903192812d40ab3dd69df98ec5']

Name

b5637231e25aa7da8fe925f5b97a2ccbfd082a5463b2a05d2b3221adb35e43d9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b5637231e25aa7da8fe925f5b97a2ccbfd082a5463b2a05d2b3221adb35e43d9']

Name

93672d67e8100bb984f866888cb042727567d302b30b91356a2b2bc8cd3f7912

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '93672d67e8100bb984f866888cb042727567d302b30b91356a2b2bc8cd3f7912']
Name
50158e22481acabc56d8e3d318d6d709fcb7a9e442e76157b518d19e13f8e520
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '50158e22481acabc56d8e3d318d6d709fcb7a9e442e76157b518d19e13f8e520']
Name
483adf61d7d932003659d5d6242eace29ea8416ec810749333793e0efa91610d
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '483adf61d7d932003659d5d6242eace29ea8416ec810749333793e0efa91610d']

Name
242851abe09cc5075d2ffdb8e5eba2f7dcf22712625ec02744eecb52acd6b1bf
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '242851abe09cc5075d2ffdb8e5eba2f7dcf22712625ec02744eecb52acd6b1bf']
Name
10b4b7e9469366bfe459c3cd674aeab0692cfd9272fe369ef56d2811623e4866
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '10b4b7e9469366bfe459c3cd674aeab0692cfd9272fe369ef56d2811623e4866']

Malware

Name
Pony - S0453
Name
Mars
Name
DarkComet - S0334
Name
Arkei Stealer
Name
Azorult - S0344
Name
QakBot - S0650
Name
Raspberry Robin

Name
LOBSHOT

Name
StealC

Name
Vidar

Name
windows

Name
azorult

Description
[Azorult](https://attack.mitre.org/software/S0344) is a commercial Trojan that is used to steal information from compromised hosts. [Azorult](https://attack.mitre.org/software/S0344) has been observed in the wild as early as 2016. In July 2018, [Azorult](https://attack.mitre.org/software/S0344) was seen used in a spearphishing campaign against targets in North America. [Azorult](https://attack.mitre.org/software/S0344) has been seen used for cryptocurrency theft. (Citation: Unit42 Azorult Nov 2018)(Citation: Proofpoint Azorult July 2018)

Name
QuackBot

Description

[QakBot](https://attack.mitre.org/software/S0650) is a modular banking trojan that has been used primarily by financially-motivated actors since at least 2007. [QakBot](https://attack.mitre.org/software/S0650) is continuously maintained and developed and has evolved from an information stealer into a delivery agent for ransomware, most notably [ProLock](https://attack.mitre.org/software/S0654) and [Egregor](https://attack.mitre.org/software/S0554).(Citation: Trend Micro Qakbot December 2020)(Citation: Red Canary Qbot)(Citation: Kaspersky QakBot September 2021)(Citation: ATT QakBot April 2021)

Name

FYNLOS

Description

[DarkComet](https://attack.mitre.org/software/S0334) is a Windows remote administration tool and backdoor.(Citation: TrendMicro DarkComet Sept 2014)(Citation: Malwarebytes DarkComet March 2018)

Name

pony

Description

[Pony](https://attack.mitre.org/software/S0453) is a credential stealing malware, though has also been used among adversaries for its downloader capabilities. The source code for Pony Loader 1.0 and 2.0 were leaked online, leading to their use by various threat actors.(Citation: Malwarebytes Pony April 2016)

Intrusion-Set

Name
Raspberry Robin

Attack-Pattern

Name
T1102
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
T1083
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

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

T1518

ID

T1518

Description

Adversaries may attempt to get a listing of software and software versions that are installed on a system or in a cloud environment. Adversaries may use the information from [Software Discovery](https://attack.mitre.org/techniques/T1518) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Adversaries may attempt to enumerate software for a variety of reasons, such as figuring out what security measures are present or if the compromised system has a version of software that is vulnerable to [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068).

Name

T1497

ID

T1497

Description

Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) during automated discovery to shape follow-on behaviors.(Citation: Deloitte Environment Awareness) Adversaries may use several methods to accomplish [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) such as checking for security monitoring tools (e.g., Sysinternals, Wireshark, etc.) or other system artifacts associated with analysis or virtualization. Adversaries may also check for legitimate user activity to help determine if it is in an analysis environment. Additional methods include use of sleep

timers or loops within malware code to avoid operating within a temporary sandbox. (Citation: Unit 42 Pirpi July 2015)

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. 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

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

T1600

ID

T1600

Description

Adversaries may compromise a network device’s encryption capability in order to bypass encryption that would otherwise protect data communications. (Citation: Cisco Synful Knock Evolution) Encryption can be used to protect transmitted network traffic to maintain its confidentiality (protect against unauthorized disclosure) and integrity (protect against unauthorized changes). Encryption ciphers are used to convert a plaintext message to ciphertext and can be computationally intensive to decipher without the associated decryption key. Typically, longer keys increase the cost of cryptanalysis, or decryption without the key. Adversaries can compromise and manipulate devices that perform encryption of network traffic. For example, through behaviors such as [Modify System Image](https://attack.mitre.org/techniques/T1601), [Reduce Key Space](https://

attack.mitre.org/techniques/T1600/001), and [Disable Crypto Hardware](https://attack.mitre.org/techniques/T1600/002), an adversary can negatively effect and/or eliminate a device's ability to securely encrypt network traffic. This poses a greater risk of unauthorized disclosure and may help facilitate data manipulation, Credential Access, or Collection efforts. (Citation: Cisco Blog Legacy Device Attacks)

Name

T1033

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

T1047

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)

Domain-Name

Value
keygenguru.com

StixFile

Value
c8d37df88009122c890cb95dc79d895d39339fe1efdcfa5e033d0aea171ffc3d
b81e857427411577552d1ecdd444efaeab23ec903192812d40ab3dd69df98ec5
b5637231e25aa7da8fe925f5b97a2ccbfd082a5463b2a05d2b3221adb35e43d9
93672d67e8100bb984f866888cb042727567d302b30b91356a2b2bc8cd3f7912
50158e22481acabc56d8e3d318d6d709fcb7a9e442e76157b518d19e13f8e520
483adf61d7d932003659d5d6242eace29ea8416ec810749333793e0efa91610d
242851abe09cc5075d2ffdb8e5eba2f7dcf22712625ec02744eecb52acd6b1bf
10b4b7e9469366bfe459c3cd674aeab0692cfd9272fe369ef56d2811623e4866

External References

- https://harfanglab.io/en/insidethelab/raspberry-robin-and-its-new-anti-emulation-trick/
- https://otx.alienvault.com/pulse/6613cc6ec22d92d374f53fd4