Apr 14 2024

NETMANAGEIT

Intelligence Report

Raspberry Robin Now Spreading Through Windows Script Files

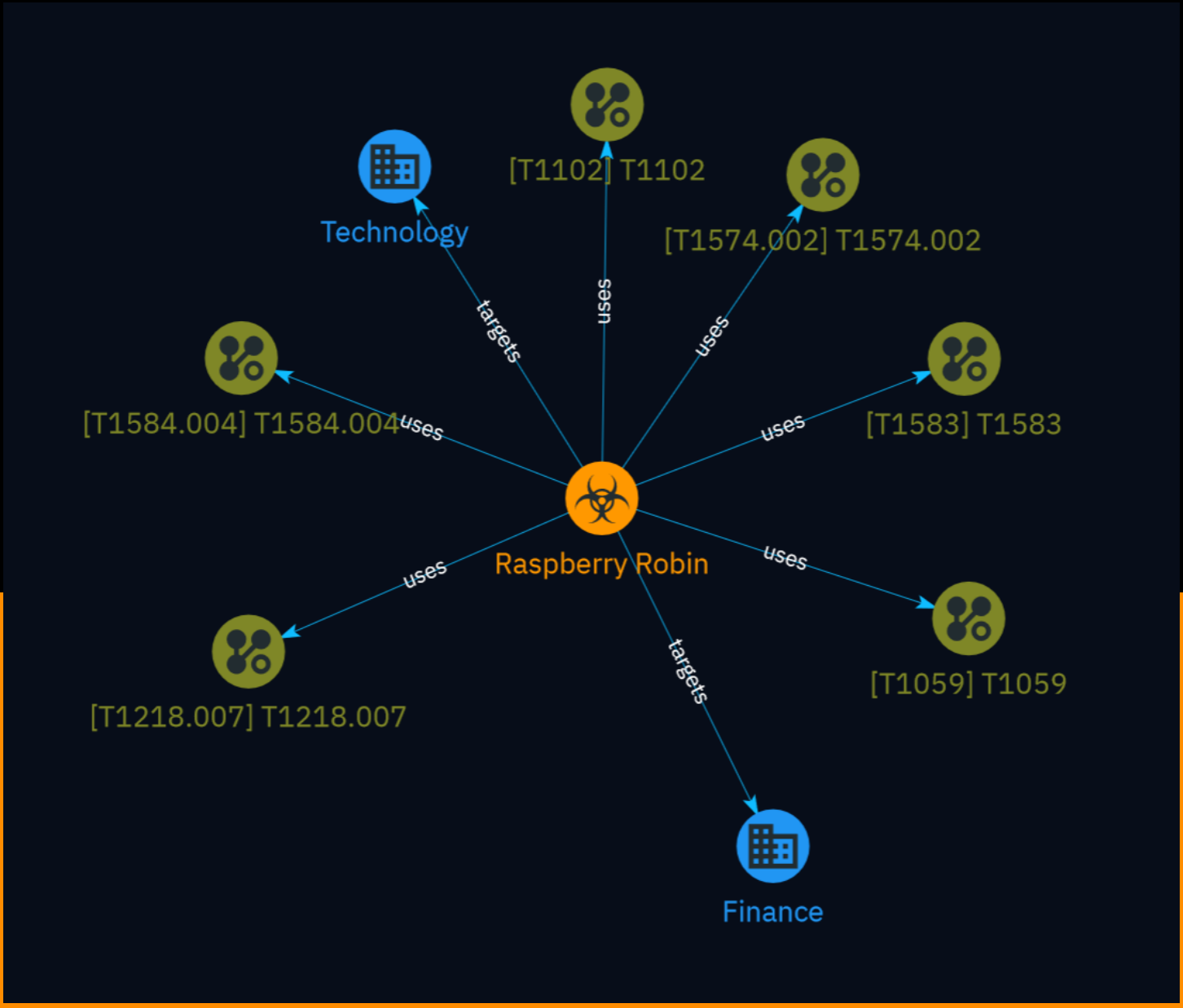

Table of contents

Overview

- Description 3
- Confidence 3
- Content 4

Entities

- Malware 5
- Attack-Pattern 6
- Sector 10

External References

- External References 11

Overview

Description

Raspberry Robin is a Windows worm initially targeting technology and manufacturing organizations. It is now spreading through highly obfuscated Windows Script Files that use anti-analysis techniques to evade detection. The scripts check the environment to avoid sandboxes before downloading the Raspberry Robin payload.

Confidence

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

100 / 100

Content

N/A

Malware

Name
Raspberry Robin

Attack-Pattern

Name
T1574.002
ID
T1574.002
Description
Adversaries may execute their own malicious payloads by side-loading DLLs. Similar to [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1574/001), side-loading involves hijacking which DLL a program loads. But rather than just planting the DLL within the search order of a program then waiting for the victim application to be invoked, adversaries may directly side-load their payloads by planting then invoking a legitimate application that executes their payload(s). Side-loading takes advantage of the DLL search order used by the loader by positioning both the victim application and malicious payload(s) alongside each other. Adversaries likely use side-loading as a means of masking actions they perform under a legitimate, trusted, and potentially elevated system or software process. Benign executables used to side-load payloads may not be flagged during delivery and/or execution. Adversary payloads may also be encrypted/packed or otherwise obfuscated until loaded into the memory of the trusted process.(Citation: FireEye DLL Side-Loading)
Name
T1584.004
ID

T1584.004

Description

Adversaries may compromise third-party servers that can be used during targeting. Use of servers allows an adversary to stage, launch, and execute an operation. During post-compromise activity, adversaries may utilize servers for various tasks, including for Command and Control. Instead of purchasing a [Server](https://attack.mitre.org/techniques/T1583/004) or [Virtual Private Server](https://attack.mitre.org/techniques/T1583/003), adversaries may compromise third-party servers in support of operations. Adversaries may also compromise web servers to support watering hole operations, as in [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), or email servers to support [Phishing](https://attack.mitre.org/techniques/T1566) operations.

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

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

T1218.007

ID

T1218.007

Description

Adversaries may abuse msiexec.exe to proxy execution of malicious payloads. Msiexec.exe is the command-line utility for the Windows Installer and is thus commonly associated with executing installation packages (.msi).(Citation: Microsoft msiexec) The Msiexec.exe

binary may also be digitally signed by Microsoft. Adversaries may abuse msiexec.exe to launch local or network accessible MSI files. Msiexec.exe can also execute DLLs.(Citation: LOLBAS Msiexec)(Citation: TrendMicro Msiexec Feb 2018) Since it may be signed and native on Windows systems, msiexec.exe can be used to bypass application control solutions that do not account for its potential abuse. Msiexec.exe execution may also be elevated to SYSTEM privileges if the `AlwaysInstallElevated` policy is enabled.(Citation: Microsoft AlwaysInstallElevated 2018)

Name

T1583

ID

T1583

Description

Adversaries may buy, lease, or rent infrastructure that can be used during targeting. A wide variety of infrastructure exists for hosting and orchestrating adversary operations. Infrastructure solutions include physical or cloud servers, domains, and third-party web services.(Citation: TrendmicroHideoutsLease) Additionally, botnets are available for rent or purchase. Use of these infrastructure solutions allows adversaries to stage, launch, and execute operations. Solutions may help adversary operations blend in with traffic that is seen as normal, such as contacting third-party web services or acquiring infrastructure to support [Proxy](https://attack.mitre.org/techniques/T1090), including from residential proxy services.(Citation: amnesty_nso_pegasus)(Citation: FBI Proxies Credential Stuffing)(Citation: Mandiant APT29 Microsoft 365 2022) Depending on the implementation, adversaries may use infrastructure that makes it difficult to physically tie back to them as well as utilize infrastructure that can be rapidly provisioned, modified, and shut down.

Sector

Name
Technology
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.
Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.

External References

- https://github.com/hpthreatresearch/iocs/blob/main/raspberryrobin/domains.txt
- https://otx.alienvault.com/pulse/6616f94c0b4d1ef52a9773f6