Play Ransomware Group Using New Custom Data-Gathering Tools

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/play-ransomware-volume-shadow-copy

```
Type type -h for help

GRB_NET  1.1.2.0

Copyright Zabbix 2022ERROR(S):

  Required option 'm, mode' is missing.

  Required option 'i, input' is missing.


-m, --mode            Required. GRB mode. scan/scanall/clr. scan -
network scanner. scanall - grab all.  clr - event logs cleaner.

-i, --input           Required. Input: f/r/s. f - file, r - range, s
- subnet, d - domain.

-d, --data            File.txt/127.0.0.1-127.0.0.255/127.0.0.1-24

-u, --username        Username for scanning

-p, --password        Password for scanning

-h, --help            (Default: ) Show help and usage.

-t, --threads         (Default: 150) Threads count. Max is 200.
Default 150.

-w, --wait            (Default: 5000) Wait time in ms. 1000 = 1s

-r, --remote_start    (Default: 0) Start remote services

-k, --domain_name     (Default: ) Domain name for Users and
Computers gathering. If not set will be used domain of current user.

--help                Display this help screen.

--version             Display version information.
```

Figure 1. Help screen displayed by Grixba malware

Scan mode

The Scan mode enumerates software and services via WMI, WinRM, Remote Registry, and Remote Services.

It then checks for the existence of the following security programs:

- Defence
- Defender
- Endpoint
- AntiVirus
- BitDefender
- Kaspersky
- Norton
- Avast

- WebRoo
- AVG
- ESET
- Malware
- Defender
- Sophos
- Trend
- Symantec Endpoint Protection
- Security
- McAfee
- TotalAV
- pcprotect
- scanguard
- Crowdstrike
- Harmony
- SentinelOne
- MVISION
- WithSecure
- WatchGuard
- FireEye
- FSecure
- Carbon Black
- Heimdal
- HitmanPro
- VIPRE
- Anti-Virus
- DeepArmor
- Morphisec
- Dr.Web

It also checks for the existence of the following backup software:

- Veeam
- Backup
- Recovery
- Synology
- C2
- Cloud
- Dropbox
- Acronis
- Cobian
- EaseUS

- Paragon
- IDrive

It then checks for the existence of the following remote administration tools:

- VNC
- Remote
- AnyDesk
- TeamViewer
- NinjaOne
- Zoho
- Atera
- ConnectWise
- RemotePC
- GoTo Resolve
- GoToAssist
- Splashtop SOS
- BeyondTrust
- Remote Desktop Manager
- Getscreen
- Action1
- Webex
- Atlassian
- Surfly
- Electric
- Pulseway
- Kaseya VSA
- XMReality
- SightCall
- DameWare
- ScreenMeet
- Viewabo
- ShowMyPC
- Iperius
- Radmin
- Remote Utilities
- RemoteToPC

Finally, it checks for the existence of the following programs:

- Hitachi Storage Navigator Modular
- .NET
- Office

- Adobe
- Word
- Excel
- Java
- Office
- Learning
- DirectX
- PowerPoint

The malware then saves all the information in CSV files and, using WinRAR, compresses them to a file named export.zip.

List of CSV files compressed by Grixba:

- alive.csv
- wm.csv
- soft.csv
- all_soft.csv
- mount.csv
- users.csv
- remote_svc.csv
- cached_RDP.csv

Scanall mode

Scanall mode is similar to Scan mode, but scans for a broader list of programs.

Clr mode

Clr mode deletes the logs from local and remote computers. It also enumerates the following registry keys:

SYSTEM\\CurrentControlSet\\services\\eventlog

SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\WINEVT\\Channels

It uses the APIs "EvtOpenLog" and "EvtClearLog" to delete the logs and deletes the WMI activity logs from the event source "Microsoft-Windows-WMI-Activity".

VSS Copying Tool

The Play ransomware gang was also recently observed using another .NET executable, which was also developed with the Costura tool.

Costura embeds the library AlphaVSS into executables. The AlphaVSS library is a.NET framework that provides a high-level interface for interacting with VSS. The library makes it easier for .NET programs to interface with VSS by offering a set of controlled APIs. Developers can use these APIs to generate, manage, and delete shadow copies, as well as access information about existing shadow copies such as size and status.

The tool created by the Play ransomware operators uses AlphaVSS to copy files from VSS snapshots. The tool enumerates the files and folders in a VSS snapshot and copies them to a destination directory. The tool allows the attackers to copy files from VSS volumes on compromised machines prior to encryption. This allows the threat actors to copy files that would normally be locked by the operating system.

Play Ransomware Background

Play ransomware (also known as PlayCrypt), which is developed by a group Symantec tracks as Balloonfly, was launched in June 2022, and since then has been responsible for multiple high-profile attacks. Like most ransomware groups now, Play carries out double-extortion attacks, where the attackers exfiltrate data from victim networks before encrypting them. While the ransomware gang had an initial focus on organizations in Latin America, especially Brazil, it soon widened its targeting.

Play is known for targeting Microsoft Exchange vulnerabilities (CVE-2022-41080, CVE-2022-41082), as well as other flaws, to gain remote code execution (RCE) and infiltrate victim networks. The group was also one of the first ransomware groups to employ intermittent encryption, a technique that allows for faster encryption of victims' systems. The tactic consists of encrypting only parts of the targeted files' content, which would still render the data unrecoverable.

Play is also notable as it doesn't appear to operate as a ransomware-as-a-service, with Balloonfly seemingly carrying out the ransomware attacks as well as developing the malware.

Use of Custom Tools on the Rise

Custom tools are increasingly being used by ransomware gangs in their attacks. This is likely due to a number of reasons, such as making attacks more efficient and reducing dwell time. Custom tools can be tailored to a specific target environment, allowing ransomware gangs to carry out attacks faster and more efficiently. The use of proprietary tools also gives ransomware operators more control over their operations. If a tool is widely available, it can be reverse-engineered or adapted by other attackers, potentially weakening the initial attack's effectiveness. By keeping their tools proprietary and exclusive, ransomware gangs can maintain their competitive advantage and maximize their profits.

Protection

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

SHA256

762bb8a7209da29afb89f7941ae1c00a04cf45a144c6c5dddcfa78ff0d941539 – Play ransomware

86e4e23f9686b129bfb2f452acb16a4c0fda73cf2bf5e93751dcf58860c6598c – SystemBC malware

f706bae95a232402488d17016ecc11ebe24a8b6cb9f10ad0fa5cbac0f174d2e7 – SystemBC malware

c59f3c8d61d940b56436c14bc148c1fe98862921b8f7bad97fbc96b31d71193c – Infostealer.Grixba

453257c3494addafb39cb6815862403e827947a1e7737eb8168cd10522465deb – Infostealer.Grixba

f71476f9adec70acc47a911a0cd1d6fea1f85469aa16f5873dd3ffd5146ccd6b – Infostealer.Grixba

a8a7fdbbc688029c0d97bf836da9ece926a85e78986d0e1ebd9b3467b3a72258 – NetScan

5ef9844903e8d596ac03cc000b69bbbe45249eea02d9678b38c07f49e4c1ec46 – NetScan

f81bd2ac937ed9e254e8b3b003cc35e010800cbbce4d760f5013ff911f01d4f9 – VSS copying tool

367d47ad48822caeedf73ce9f26a3a92db6f9f2eb18ee6d650806959b6d7d0a2 – WinRAR

6f95f7f53b3b6537aeb7c5f0025dbca5e88e6131b7453cfb4ee4d1f11eeaebfc – WinSCP

1409e010675bf4a40db0a845b60db3aae5b302834e80adeec884aebc55eccbf7 – PsExec

Network

137.220[.]49.66 – SystemBC C&C

justiceukraine.com – SystemBC C&C