Ransomware Spotlight: Play

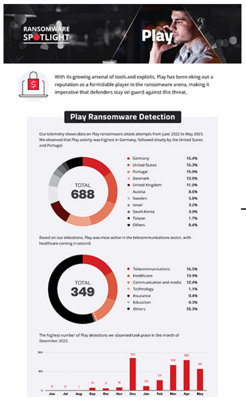
trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-play

X

Play

By Trend Micro Research

Play is shaping up to be a player on the rise within the ransomware landscape, with its operators likely to continue using the ransomware in future. We take a deep dive into its operations and offer ways in which organizations can shore up their defenses against this emerging threat.



With its growing arsenal of tools and exploits, Play has been eking out a reputation as a formidable player in the ransomware arena, making it imperative that defenders stay on guard against this threat.

Play Ransomware Detection

Our telemetry shows data on Play ransomware attack attempts from June 2022 to May 2023. We observed that Play activity was highest in Germany, followed closely by the United States and Portugal.

Based on our detections, Play was most active in the telecommunications sector, with healthcare coming in second.

The highest number of Play detections we observed took place in the month of December 2022.

_View infographic of "Ransomware Spotlight: Play"

In July 2022, our researchers looked into ransomware cases in Latin America that targeted government entities and were initially attributed to a newcomer called Play ransomware, which derives its name based on its behavior: it adds the extension ".play" after encrypting files. Similarly, its ransom note contains the single word "PLAY", along with the ransomware group's email address. In June 2022, victims of Play ransomware initially surfaced on Bleeping Computer forums, and a month later, the "No-logs No breach" website provided further details on this ransomware.

Over the course of our investigation, the threat actors running Play ransomware have added more tools and abused new vulnerabilities to their growing arsenal. This suggests that the ransomware group continues to refine its playbook of tactics, techniques, and procedures (TTPs), intending to remain active on the scene for the foreseeable future.

What organizations need to know about Play

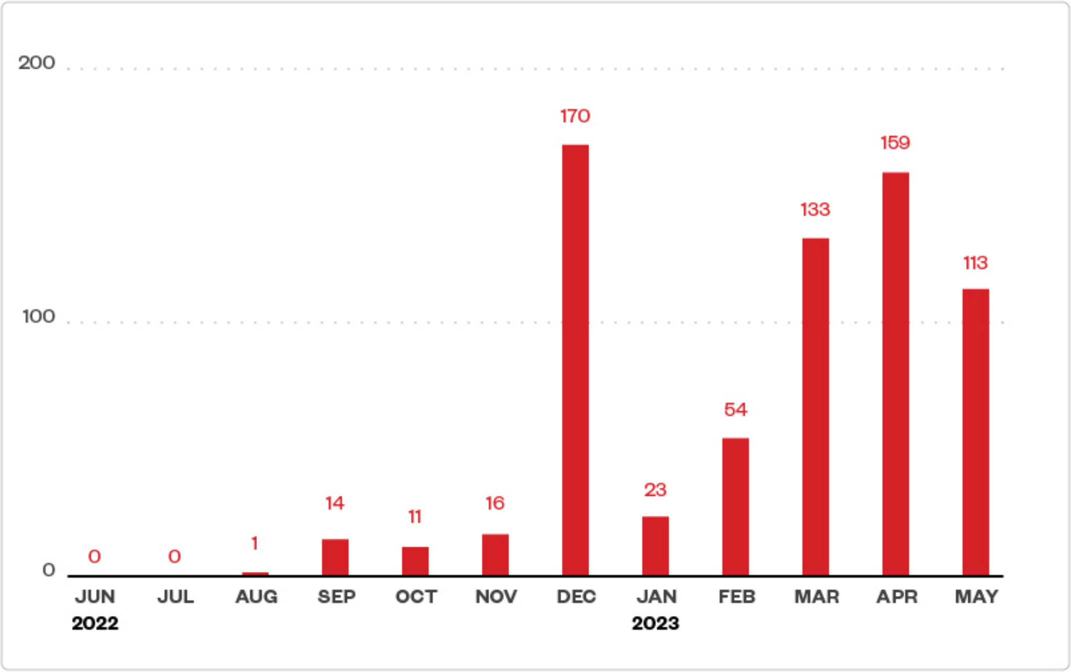
We have observed the Play ransomware group augmenting their toolbox with a number of new tools and exploits, including the vulnerabilities ProxyNotShell, OWASSRF, and a Microsoft Exchange Server Remote Code Execution. More recently, it's also begun to use new tools like Grixba, a custom network scanner and infostealer, and the open-source VSS management tool AlphaVSS.

We have also found evidence that suggests a possible link between Play ransomware and various ransomware families: It shares some tactics and tools with Hive and Nokoyawa ransomware, for example, that point to a high likelihood of affiliation between these ransomware families. We intend on validating the related URLs from Play ransomware infections in terms of watermarking in order to confirm any relation to past Hive infections, as was done previously with Nokoyawa infections.

There are also some notable similarities between Play and Quantum ransomware, an offshoot of the Conti ransomware group, inasmuch as the two ransomware groups partly share the same infrastructure: Play's attacks use Cobalt Strike beacons that have the same watermark, 206546002, as with those that had been dropped by Emotet and SVCReady botnets in Quantum ransomware attacks. Despite there being no spam campaigns that are currently using the Emotet trojan, over the course of our investigation we have detected select cases in which Emotet was used to deploy Cobalt Strike beacons bearing the same 206546002 watermark that were found in the beacons involved in Play's ransomware attacks.

Top affected industries and countries

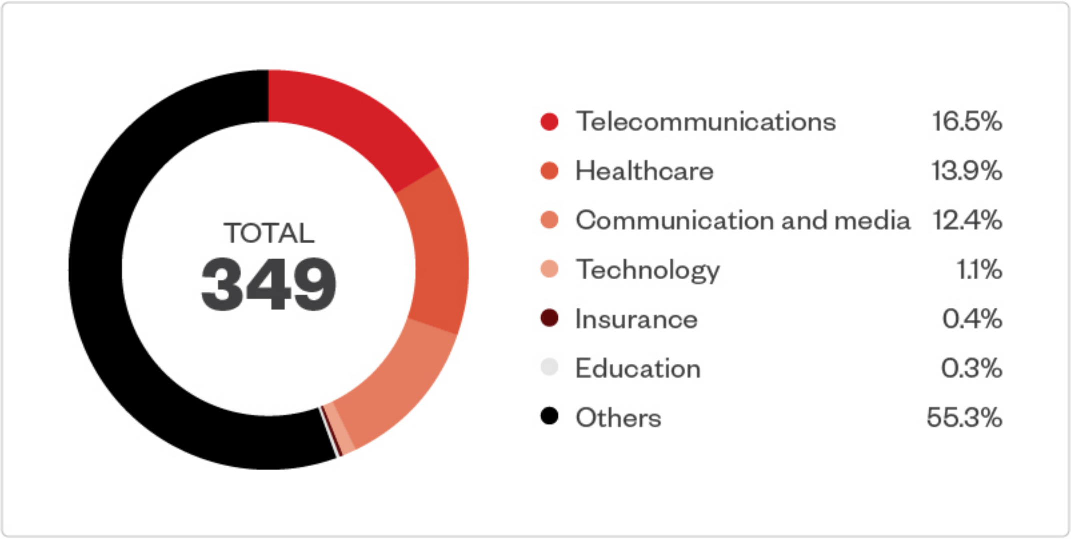
In this section, we examine Play ransomware's attempts to compromise organizations from June 2022 to May 2023 based on Trend's Smart Protection Network™ country and regional data. It's important to note that this data covers only Trend customers and does not contain all victims of Play ransomware. In that time period, Play ransomware activity climbed steadily, peaking in December 2022 with 170 attack attempts.



©2023 TREND MICRO

Figure 1. A monthly breakdown of detected Play ransomware attempted attacks in terms of infected machines (June 2022 - May 2023)
Source: *Trend's Smart Protection Network™*

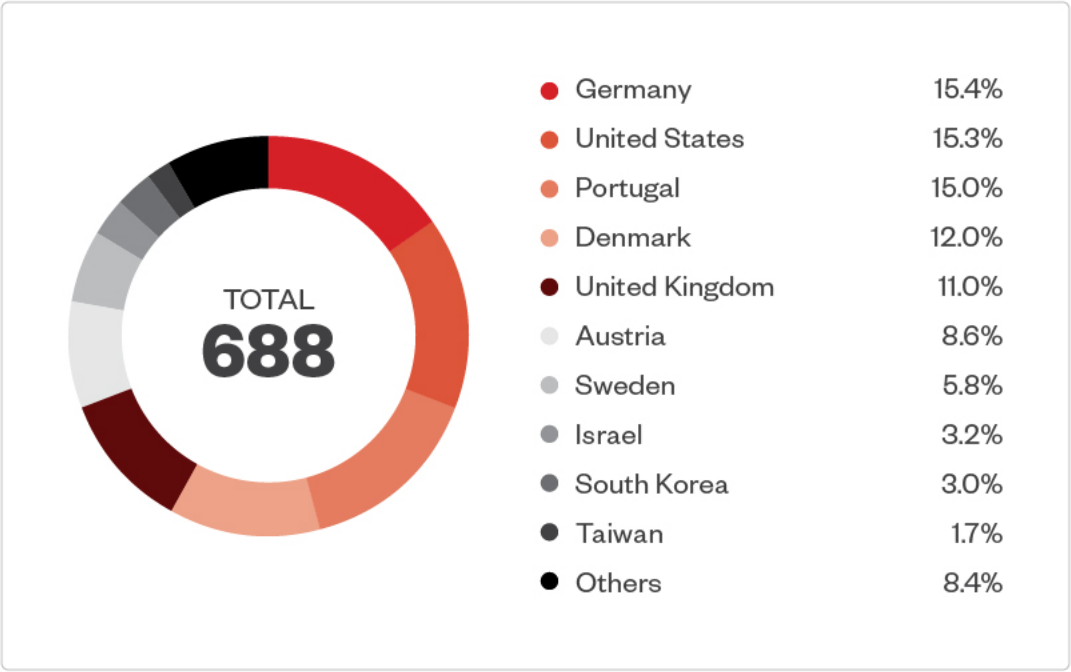
Data from customers who specified their industries showed that Play ransomware appeared most active in the telecommunications sector. The healthcare, and communication and media sectors were also highly targeted.



©2023 TREND MICRO

Figure 2. Industries with the highest number of attack attempts in terms of infected machines for Play ransomware (June 2022 - May 2023)
Source: *Trend's Smart Protection Network™*

Our telemetry also shows that the heaviest concentration of Play ransomware attack attempts was made against organizations located in Germany, which composed 15.4% of the total detections. This is followed closely by the United States and Portugal, at 15.3% and 15%, respectively.



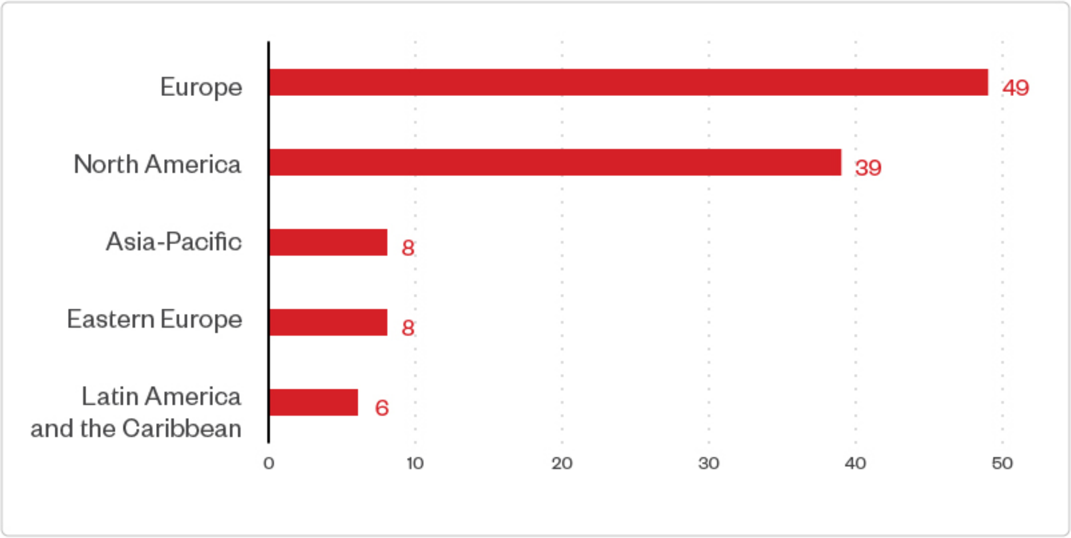
©2023 TREND MICRO

Figure 3. Countries with the highest number of attack attempts in terms of infected machines for Play ransomware (June 2022 - May 2023)
Source: *Trend's Smart Protection Network™*

Targeted regions and industries according to Play leak site

This section looks at data based on attacks recorded on the leak site of the operators behind Play ransomware from June 2022 to May 2023. Based on both Trend's open-source intelligence (OSINT) research and investigations into the leak site, Play ransomware actors had managed to compromise a total of 110 victims who refused to pay the ransom demand as of this writing.

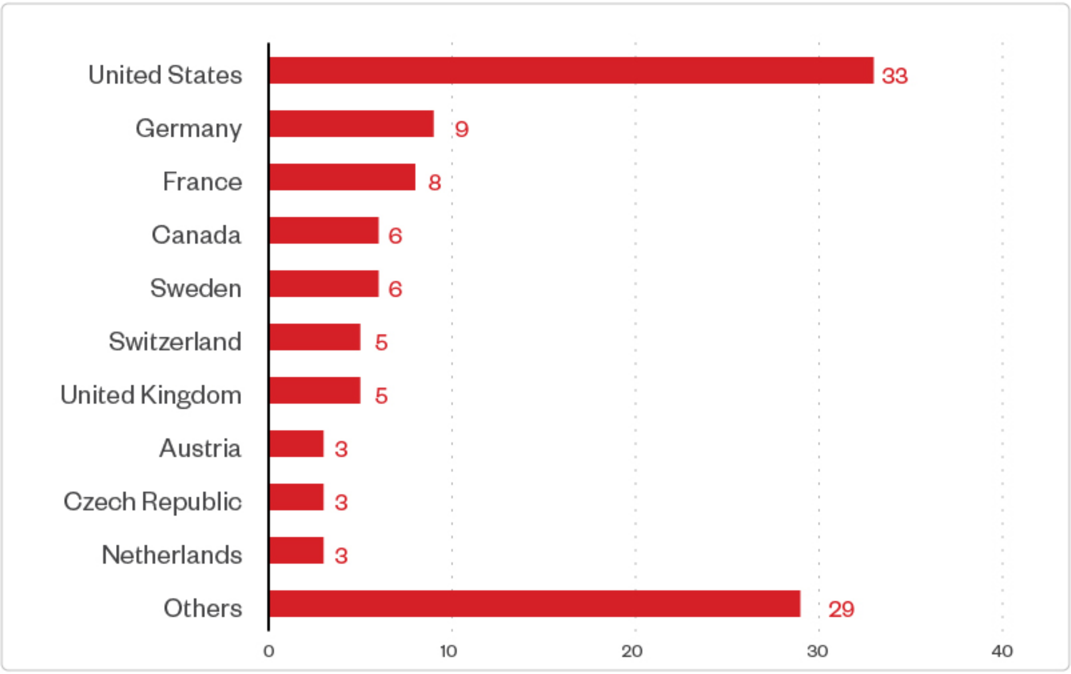
Organizations based in Europe were the hardest hit among the victims identified in Play's leak site at 49 attacks; those in North America came in second at 39. More specifically, the United States was at the receiving end of most of the attacks, with 33 affected organizations. Many confirmed ransomware attacks also took place in Germany and France, with 9 and 8 victims respectively.



©2023 TREND MICRO

Figure 4. The distribution by region of Play ransomware's victim organizations (June 2022 - May 2023)
Sources: *Play ransomware's leak site and Trend's OSINT research*

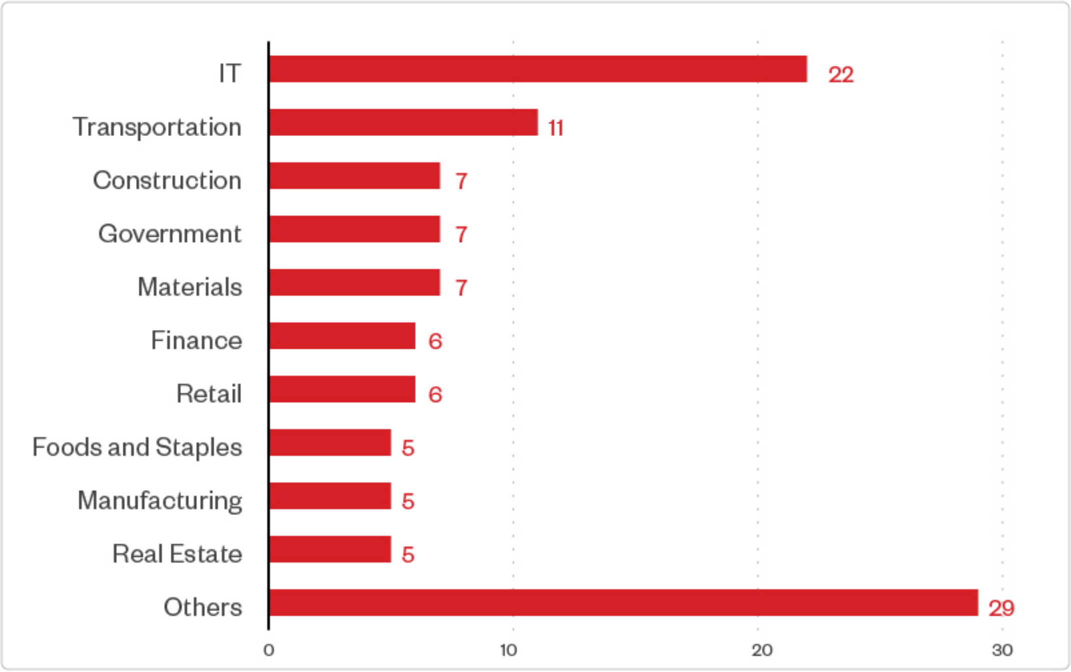
The leak site data indicates that the IT industry was most targeted by Play's attacks, followed by transportation. Other affected organizations include those in the construction and materials industry, as well as government entities.



©2023 TREND MICRO

Figure 5. The top 10 countries most targeted by Play ransomware threat actors (June 2022 - May 2023)
Sources: *Play ransomware's leak site and Trend's OSINT research*

Most of Play ransomware's victim organizations were small-sized businesses. However, a number of affected organizations did not have their sizes specified.



©2023 TREND MICRO

Figure 6. The top 10 industries most targeted by Play ransomware threat actors (June 2022 - May 2023)
Sources: *Play ransomware's leak site and Trend's OSINT research*

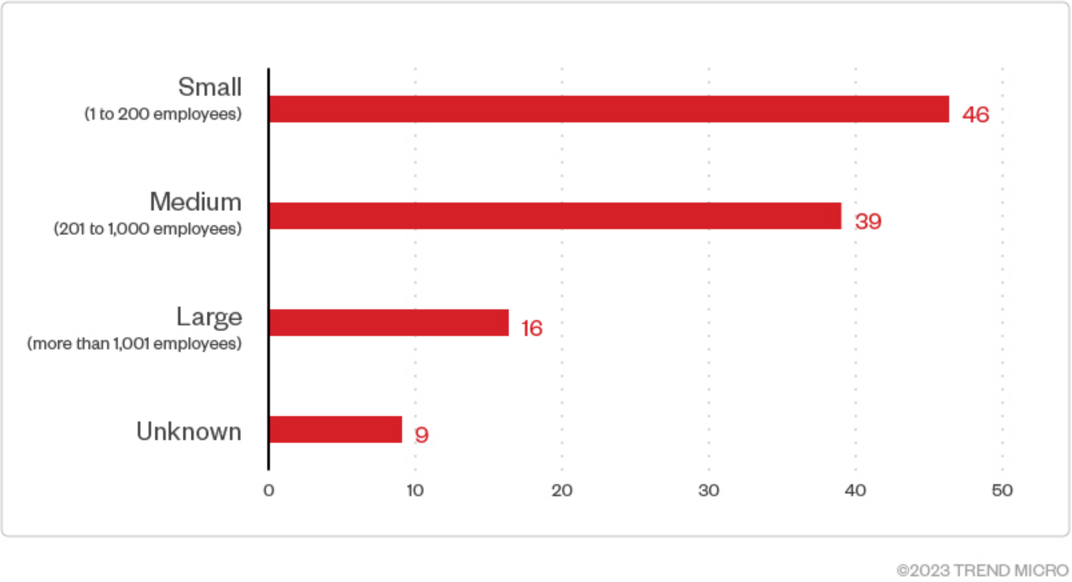


Figure 7. The distribution by organization size of Play ransomware's victim organizations (June 2022 - May 2023)
Sources: *Play ransomware's leak site and Trend's OSINT research*

Infection chain and techniques

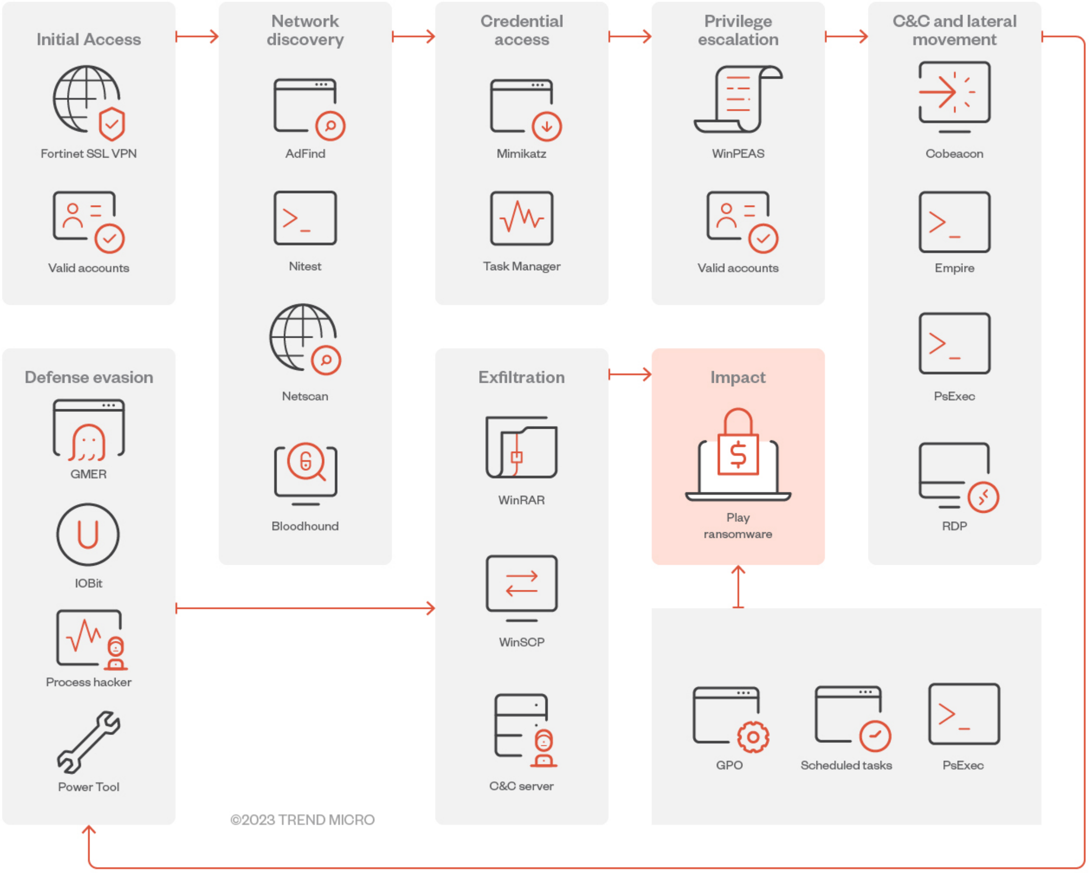


Figure 8. Play ransomware's infection chain

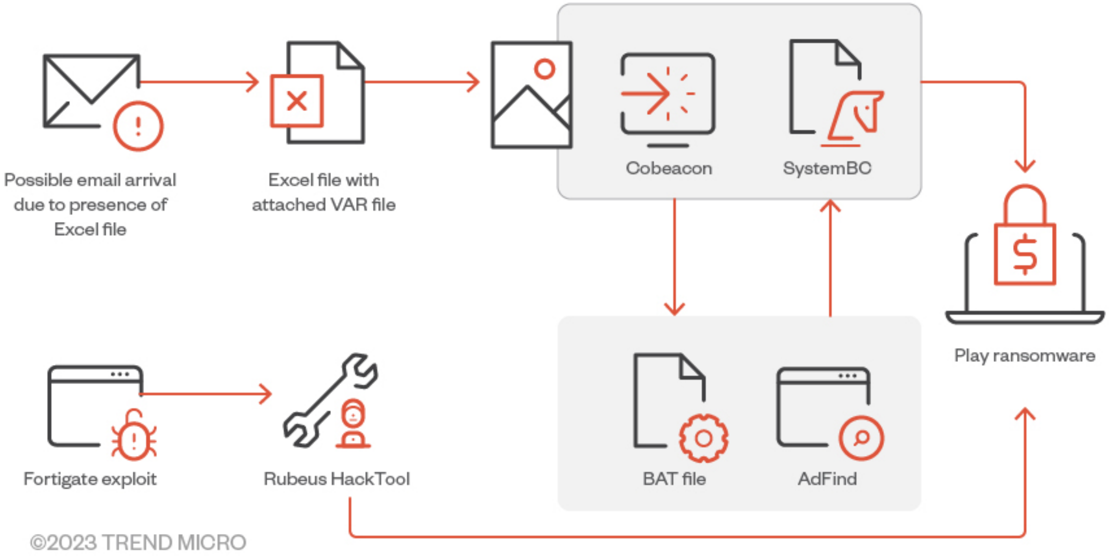


Figure 9. Play ransomware's infection chain observed in another campaign

Initial Access

- The actors behind Play ransomware usually achieve initial access by way of valid accounts – including virtual private network (VPN) accounts, not just domain and local accounts – that have been reused across multiple platforms, previously exposed, or obtained by illegal means. To establish a foothold into their targeted system, they also use exposed remote desktop protocol (RDP) servers.
- Additionally, Play ransomware exploited two FortiOS vulnerabilities: CVE-2018-13379, a path traversal vulnerability in the FortiOS SSL VPN web portal that allows an unauthenticated attacker to download OS system files through specially crafted HTTP resource requests; and CVE-2020-12812, an improper-authentication vulnerability in SSL VPN in FortiOS that allows a user to log in without being prompted for the second factor of authentication, FortiToken, if they changed the case of their username.
- Play ransomware has also used new CVEs to gain initial access: These include ProxyNotShell (CVE-2022-41040), a server-side request forgery (SSRF) vulnerability that allows an authenticated attacker to remotely trigger the next vulnerability, CVE-2022-41082; OWASSRF (CVE-2022-41080), a new exploit method for Microsoft Exchange Server after the patch for ProxyNotShell; and Microsoft Exchange Server Remote Code Execution (CVE-2022-41082), a follow-up exploit to ProxyNotShell and OWASSRF designed to achieve RCE using the respective PowerShell endpoints of each vulnerability.

Privilege Escalation

Using Mimikatz, Play ransomware extracts high privileges credentials from memory, after which it adds accounts to privileged groups, including the Domain Administrators group. It uses Windows Privilege Escalation Awesome Scripts (WinPEAS), a script that searches for possible local privilege escalation paths, to perform vulnerability enumeration.

Defense evasion

- Play ransomware disables antimalware and monitoring solutions using tools like Process Hacker, GMER, IOBit, and PowerTool. It covers its tracks using the Windows built-in tool wevtutil or a batch script as a means of removing indicators of its presence, including logs in Windows Event Logs or malicious files.
- In June, we also observed some Play attacks that specifically targeted Microsoft Defender by disabling its real-time monitoring and antivirus protection capabilities. Through PowerShell or command prompt, it disables Micosoft Defender's protection capabilities. The PowerShell scripts that Play ransomware uses, like Cobalt Strike beacons (Cobeacon) or Empire agents, are encrypted in Base64.

Discovery

Play ransomware's actors gather more details about the Active Directory (AD) environment in the discovery phase of their attacks. We found that AD queries for remote systems were performed by different tools like ADFind, Microsoft Nltest, Bloodhound. Grixba is also used to check for a list of security files and processes, among others. The ransomware operators also performed the enumeration of system information, such as hostnames, shares, and domain information.

Credential Access

Play ransomware uses Mimikatz – a tool that can be dropped directly on the target host or executed as a module through a command-and-control (C&C) application like Empire or Cobalt Strike – to dump credentials. The malware also the Windows tool Task Manager as a means of dumping the Local Security Authority Subsystem Service (LSASS) process from memory. Another one of its discovery tools is the Grixba infostealer, which Play ransomware uses to check for a list of security files and processes, among others.

Lateral Movement

Play ransomware may use different tools to move laterally across a victim's system:

- Cobalt Strike SMB beacon, which is used as a C&C beacon, a method of lateral movement, and a tool for downloading and executing files
- SystemBC, a SOCKS5 proxy bot that serves as a backdoor with the ability to communicate over TOR, is used for backdooring mechanisms
- Empire, an open-source post-exploitation framework that's used to conduct Play ransomware's post-exploitation activity
- Mimikatz, which is used to dump credentials and gain domain administrator access on victim networks to conduct lateral movement

Exfiltration

A victim's data is often split into chunks instead of using whole files prior to exfiltration, which Play ransomware may do so as to avoid triggering network data transfer. Play ransomware utilizes WinSCP, an SFTP client and FTP client for Microsoft Windows. WinRAR is also used to compress the files in .RAR format for later exfiltration. A web page developed in PHP is used to receive the exfiltrated files.

Impact

After encrypting a file, Play adds the ".play" extension to that file. A ransom note titled ReadMe.txt is created in the hard drive root (C:). The ransom notes among all the cases we investigated contained an email address that followed the same format: [seven random characters]@gmx[.]com. It also uses AlphaVSS to delete shadow copies, which disables the victim machine's System Restore capability.

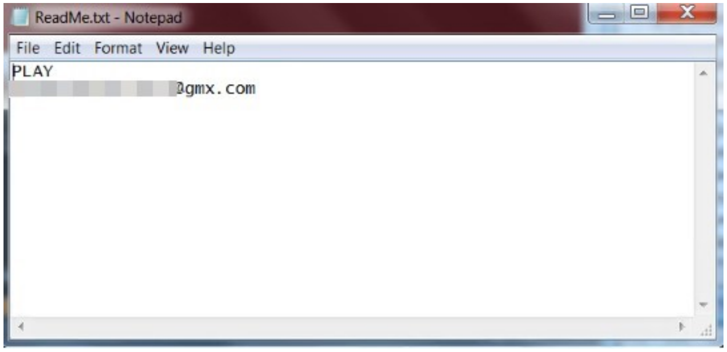
Other technical details

- Play encrypts files with the following extensions:
    - .$er
    - .4dd
    - .4dl
    - .abcddb
    - .abs
    - .abx
    - .ac
    - .accdb
    - .accdc
    - .accde
    - .accdr
    - .accdt
    - .accdw
    - .accft
    - .adb
    - .ade
    - .adf
    - .adn
    - .adp
    - .alf
    - .anb
    - .aq
    - .arc
    - .ask
    - .bak
    - .bcp
    - .bdf
    - .btr
    - .cat
    - .cdb
    - .ckp
    - .cma
    - .cpd
    - .crypt
    - .crypt1
    - .crypt10
    - .crypt12
    - .crypt14
    - .crypt15
    - .crypt5
    - .crypt6
    - .crypt7
    - .crypt8
    - .crypt9
    - .dacpac
    - .dad
    - .daschema
    - .dat
    - .db
    - .db-shm
    - .db-wal
    - .db2
    - .db3
    - .dbc
    - .dbcrypt
    - .dbcrypt8
    - .dbf
    - .dbs
    - .dbt
    - .dbv
    - .dbx
    - .dcb

- .dct
- .dcx
- .ddl
- .dlis
- .dp1
- .dqy
- .dsk
- .dsn
- .dtsx
- .dxl
- .eco
- .ecx
- .edb
- .epim
- .exb
- .fcd
- .fdb
- .fic
- .fm5
- .fmp
- .fmp12
- .fmpsl
- .fol
- .fp3
- .fp4
- .fp5
- .fp7
- .fpt
- .frm
- .gdb
- .grdb
- .gwi
- .hdb
- .his
- .hjt
- .ib
- .ibd
- .icg
- .icr
- .idb
- .ihx
- .itdb
- .itw
- .jet
- .jtx
- .kdb
- .kexi
- .kexic
- .kexis
- .ldf
- .lgc
- .log1
- .luminar
- .lut
- .lwx
- .maf
- .maq
- .mar
- .mas
- .mav
- .maw
- .mdb
- .mdf

- .mdn
- .mdt
- .mpd
- .mrg
- .mud
- .mwb
- .myd
- .myi
- .ndf
- .ns2
- .ns3
- .ns4
- .nsf
- .nv
- .nv2
- .nwdb
- .nyf
- .odb
- .oqy
- .ora
- .orx
- .owc
- .p96
- .p97
- .pan
- .pdb
- .pdm
- .pnz
- .qry
- .qvd
- .rbf
- .rctd
- .rod
- .rodx
- .rpd
- .rsd
- .sav
- .sbf
- .scx
- .sdb
- .sdc
- .sdf
- .sdy
- .sis
- .spq
- .sql
- .sqlite
- .sqlite3
- .sqlitedb
- .te
- .temx
- .tmd
- .tps
- .trc
- .trm
- .udb
- .udl
- .usr
- .v12
- .vis
- .vpd
- .vvv
- .wdb

    - .wmdb
    - .wrk
    - .xdb
    - .xld
    - .xmlff
- Avoids the following directories/drive types:
    - RAM Disk
    - CD-ROM Drive
- It avoids encrypting files with these strings in their file name:
    - ReadMe.txt
    - bootmgr
- It avoids encrypting files with the following extensions:
    - .PLAY
    - .exe
    - .msi
    - .dll
    - .lnk
    - .sys
- An example of a dropped ransom note in a Play ransomware attack:



```
PLAY
[redacted]@gmx.com
```

Figure 10. Play ransomware’s dropped ransom note

- Encryption Method

    AES-RSA Hybrid Encryption
- Hacktools
    - Cobalt Strike
    - Webshells
    - Adfind
    - Batch Files
    - SystemBC
    - Powertool64
    - Psexec

MITRE tactics and techniques

Initial Access	**Execution**	**Defense Evasion**	**Credential Access**	**Discovery**	**Lateral Movement**	**Command and Control**	**Exfiltration**	**Impact**

Initial Access	Execution	Defense Evasion	Credential Access	Discovery	Lateral Movement	Command and Control	Exfiltration	Impact
T1190 - Exploit Public-Facing Application *Has been observed to be using several exploits as part of its entry vector:* *• FortiOS SSL VPN Exploits (CVE-2018-13379 and CVE-2020-12812)* *• ProxyNotShell (CVE-2022-41040)* *• OWASSRF (CVE-2022-41080)* *• MS Exchange Server Remote Code Execution (CVE-2022-41082)* *Some reports also mention arriving via spam mail*	**T1059** - Command and Scripting Interpreter *Uses several scripts like PowerShell and batch files as part of its execution and other functionalities* **T1203** - Exploitation for Client Execution *Combined with some of the exploits used as initial access, another exploit is used to download and execute other components:* *• MS Exchange Server Remote Code Execution (CVE-2022-41082)*	**T1562** - Impair Defenses *Makes use of third-party tools like GMER, Process Hacker, PowerTool, and so on, to try and disable antivirus-related services and processes like Microsoft Defender* **T1140** - Deobfuscate/Decode Files or Information *Makes use of obfuscated codes and/or files to try and avoid detection or make it harder for analysis* **T1070** - Indicator Removal *May sometimes delete itself or components to avoid leaving indication of compromise*	**T1003** - OS Credential Dumping **T1552** - Unsecured Credentials *Makes use of Mimikatz to dump credentials*	**T1033** - System Owner/User Discovery **T1082** - System Information Discovery **T1083** - File and Directory Discovery **T1135** - Network Share Discovery **T1057** - Process Discovery **T1007** - System Service Discovery *Using its remote access tools (RATs) and/or the ransomware binary itself, Play can discover several system information such as:* *• Users* *• OS information* *• Files and directory* *• Accessible system within the compromised network* *• Running processes* *• Running services* *It also uses the Grixba infostealer as a tool for discovery.*	**T1021** - Remote Services: SMB/Windows Admin Shares *Upon discovery of available network shares, it can use this to traverse the network via SMB*	**T1071** - Application Layer Protocol *Connects to its C&C server via typical protocols, such as HTTP and HTTPS*	**T1002** - Data Compressed *Uses archiving tools like WinRar to compress stolen data or files to prepare these for exfiltration* **T1048** - Exfiltration Over Alternative Protocol *Can either exfiltrate via its own C&C server or makes use of file transfer tools like WinSCP*	**T1486** - Data Encrypted for Impact *Play ransomware uses intermittent encryption and the hybrid AES-RSA encryption method* **T1489** - Service Stop *Can disable antivirus-related services* **T1490** - Inhibit System Recovery *Uses AlphaVSS to inhibit system recovery*

Summary of malware, tools, and exploits used

Security teams should keep an eye out for the presence of these malware tools and exploits that are typically used in Play's ransomware attacks:

Initial Access	Execution	Discovery	Credential Access	Lateral Movement	Defense Evasion	Exfiltration	Impact

Initial Access	Execution	Discovery	Credential Access	Lateral Movement	Defense Evasion	Exfiltration	Impact
FortiOS SSL VPN Exploits (CVE-2018-13379 and CVE-2020-12812)	Cobeacon	Adfind	Mimikatz	Cobeacon	GMER	WinRAR	AlphaV
ProxyNotShell (CVE-2022-41040)	SystemBC	Bloodhound		PsExec	IOBit	WinSCP	
OWASSRF (CVE-2022-41080)		Grixba		PowerShell Empire	Process Hacker		
MS Exchange Server Remote Code Execution (CVE-2022-41082)		Netscan		RDP	PowerTool		
		NlTest					

Security Recommendations

<

Our analysis of Play ransomware underscores the great strides modern threat actors have since taken to design attacks that are better equipped to go under the radar and avoid detection. In light of this, organizations should stay vigilant of ransomware actors that have turned to red-team or penetration-testing tools as a means of camouflaging their presence when infiltrating their targeted systems.

In defending systems against threats like Play ransomware, organizations can benefit from establishing security frameworks that can allocate resources systematically for establishing solid defenses against ransomware. Here are some best practices that can be included in these frameworks:

Audit and inventory

- Take an inventory of assets and data.
- Identify authorized and unauthorized devices and software.
- Make an audit of event and incident logs.

Configure and monitor

- Manage hardware and software configurations.
- Grant admin privileges and access only when necessary to an employee’s role.
- Monitor network ports, protocols, and services.
- Activate security configurations on network infrastructure devices such as firewalls and routers.
- Establish a software allowlist that executes only legitimate applications.

Patch and update

- Conduct regular vulnerability assessments.
- Perform patching or virtual patching for operating systems and applications.
- Update software and applications to their latest versions.

Protect and recover

- Implement data protection, backup, and recovery measures.
- Enable multifactor authentication (MFA).

Secure and defend

- Employ sandbox analysis to block malicious emails.
- Deploy the latest versions of security solutions to all layers of the system, including email, endpoint, web, and network.
- Detect early signs of an attack such as the presence of suspicious tools in the system.
- Use advanced detection technologies such as those powered by AI and machine learning.

Train and test

- Regularly train and assess employees on security skills.
- Conduct red-team exercises and penetration tests.

A multilayered approach can help organizations guard possible entry points into the system (endpoint, email, web, and network). Security solutions that can detect malicious components and suspicious behavior can also help protect enterprises.

- Trend Micro Vision One™ provides multilayered protection and behavior detection, which helps block questionable behavior and tools early on before the ransomware can do irreversible damage to the system.
- Trend Micro Cloud One™ Workload Security protects systems against both known and unknown threats that exploit vulnerabilities. This protection is made possible through techniques such as virtual patching and machine learning.
- Trend Micro™ Deep Discovery™ Email Inspector employs custom sandboxing and advanced analysis techniques to effectively block malicious emails, including phishing emails that can serve as entry points for ransomware.
- Trend Micro Apex One™ offers next-level automated threat detection and response against advanced concerns such as fileless threats and ransomware, ensuring the protection of endpoints.

Indicators of Compromise (IOCs)

The IOCs for this article can be found here. Actual indicators might vary per attack.

HIDE

Like it? Add this infographic to your site:
1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.