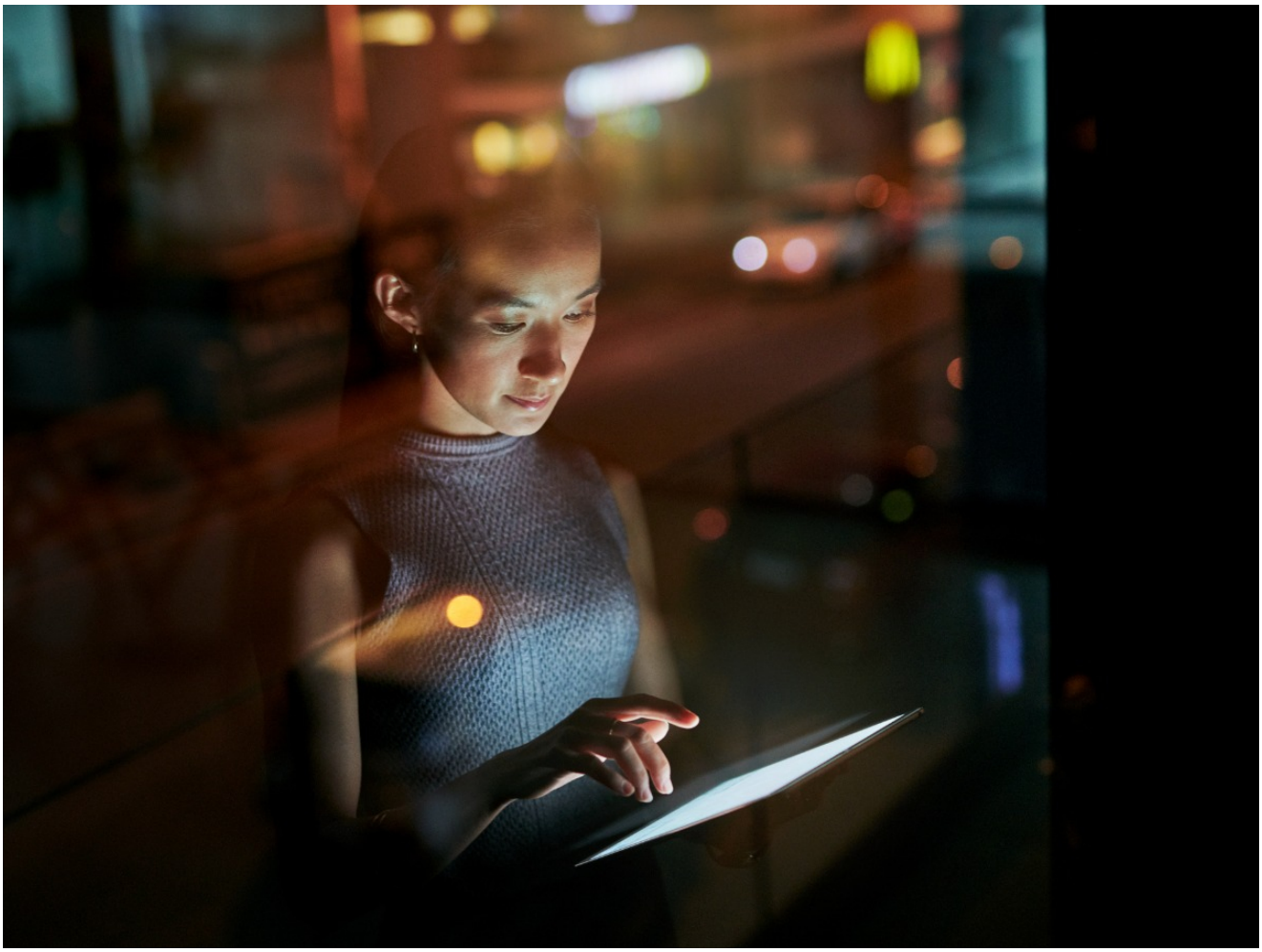
Ransomware Roundup – Play Ransomware

fortinet.com/blog/threat-research/ransomware-roundup-play-ransomware

December 22, 2022



On a bi-weekly basis, FortiGuard Labs gathers data on ransomware variants of interest that have been gaining traction within our datasets and the OSINT community. The Ransomware Roundup report aims to provide readers with brief insights into the evolving ransomware landscape and the Fortinet solutions that protect against those variants.

This latest edition of the Ransomware Roundup covers the Play ransomware.

Affected platforms: Microsoft Windows
Impacted parties: Microsoft Windows Users
Impact: Encrypts files on the compromised machine and demands ransom for file decryption
Severity level: High

Play Ransomware Overview

Play is a relative newcomer to the ransomware game, having been detected for the first time in June 2022. In this report, Play refers to both the group developing and distributing it and the name of the ransomware executable. Like many other operators in this space, Play has adopted the double-extortion methodology of encrypting endpoints and/or other infrastructure of value within an organization and then threatening to release exfiltrated data from those machines on the internet if a ransom is not paid.

Play Ransomware Infection Vector

Play has been seen to use a number of common methods to gain access to an environment, including phishing, valid compromised accounts, and exposed RDP (Remote Desktop Protocol) servers. Once a beachhead has been established, LOLBINS (Living Off the Land Binaries) are used to explore and then prepare the ground to execute malware on machines of interest.

Play Ransomware Executable

The ransomware executable is Microsoft Visual C++ based and contains several anti-debugging and anti-analysis features to slow investigations into the activity of the malware. These features include garbage code (untethered instructions that serve no useful purpose) and function returns that drive execution into a dead end.

Figure 1. Garbage code in the Play executable.

Play Ransomware Execution

When launched, the ransomware encrypts all files of interest, such as personal and operational documents (it does not touch system files), and leaves them with a ".PLAY" extension.

Figure 2. Files encrypted by Play.

When encryption is complete, a ransom note named "ReadMe.txt" is added to the root of the primary drive (e.g., C:\). This note contains a link to the group's TOR pages and a contact e-mail address.

Figure 3. Play ransom note.

The "Play News" landing page lists the companies allegedly impacted by Play and a countdown to the possible release of any data gathered by them. Organizations that have refused to pay also have links to their data posted here.

There is also a contact portal where the group can be reached, an "FAQ" section that broadly describes what the group has done, and steps for victims to take to restore their data.

Figure 4. Play TOR “News” countdown page.

Figure 5. Play TOR “News” contact page.

Figure 6. Play TOR “News” FAQ page.

As of this writing, the “Play News” page lists seven active victims currently being threatened. The regional breakdown of the victims is below:

Figure 7. Active Victim Counts by Region

The regional breakdown of victims whose stolen data was leaked is as follows:

Figure 8. Previous Victim Counts by Region

Based on this information, the Play ransomware threat actors appear to target victims regardless of their region. The one caveat is that enterprises in former Soviet states do not appear to be listed on “Play News”, although this may be coincidental.

Fortinet Protection

Fortinet customers are already protected from this malware variant through FortiGuard’s Web Filtering, AntiVirus, and FortiEDR services, as follows:

FortiGuard Labs detects known Play ransomware variants with the following AV signatures:

- W32/Filecoder.PLAY!tr.ransom
- W32/Filecoder_PLAY.B!tr
- W32/Filecoder.OLT!tr.ransom
- W32/Filecoder.NHQDTEZ!tr.ransom
- Riskware/Filecoder_PLAY
- W32/PossibleThreat

IOCs

File-based IOCs:

SHA256
f18bc899bcacd28aaa016d220ea8df4db540795e588f8887fe8ee9b697ef819f
e641b622b1f180fe189e3f39b3466b16ca5040b5a1869e5d30c92cca5727d3f0

608e2b023dc8f7e02ae2000fc7dbfc24e47807d1e4264cbd6bb5839c81f91934

006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55

e4f32fe39ce7f9f293ccbfde30adfdc36caf7cfb6ccc396870527f45534b840b

8962de34e5d63228d5ab037c87262e5b13bb9c17e73e5db7d6be4212d66f1c22

5573cbe13c0dbfd3d0e467b9907f3a89c1c133c774ada906ea256e228ae885d5

f6072ff57c1cfe74b88f521d70c524bcbbb60c561705e9febe033f51131be408

7d14b98cdc1b898bd0d9be80398fc59ab560e8c44e0a9dedac8ad4ece3d450b0

dcaf62ee4637397b2aaa73dbe41cfb514c71565f1d4770944c9b678cd2545087

f5c2391dbd7ebb28d36d7089ef04f1bd9d366a31e3902abed1755708207498c0

3e6317229d122073f57264d6f69ae3e145decad3666ddad8173c942e80588e69

dd101db5d9503f33a0c23d79da3642e999375748f7c1532e98c813b114bdfa1a

47c7cee3d76106279c4c28ad1de3c833c1ba0a2ec56b0150586c7e8480ccae57

703075181922eb8db8d23279eaed8f7263dfa2b64383cff675da4cedc2394af5

f39d6741cbb99a81decbe5e75c07e846b5a36b40bc1bb0c0c61415300cc43b6c

8d94028bfaac5bef84c56b01f40e429ae4cdf799b2b755dfba9eee3b72448b5b

f0a3047e9d557e2150501e302d5e96a1c2669858fb0072f97024fe0dd07d5271

8556dfe5582a5647a5e96cd77e6239874504a01a9c7b9e512e70329ec6f61aea

5e94626c6bcb825acede3826811ed693644d6dbb7caeeefb8575c2ec711a65a6

a29e20d89e8c933e05b690b2779f82716fb31f688594b99d868e4382058caa8f
757524b09e5d4f2399172c4ac0f6996ec34dec90110542973d438d5370aff280
3a36e917a4a6587290a393d5b10d0bd42f99cf0c72a2e7de751a4bfaeb9d30c5
92f3abed62d710064a19f2a50c4482cd02adfd821ace4c2f3030f96290166189
157c43a3a4e014827e42cf4dd20cc8efa71cdf098f5d1d04b6cd1a972d6a8c7a
5eca08ddca898427de5ab13fedf25426102c3a0621d086b63f2e37d2d04ba3e9
2b4111121fb35b46665c42e3ea2cf1b8eda5afce580e310465cb259bb1abd053
12d1a0dc37d877dbf81bd18e8bd57b2843cc254c9a3cfcbecb70305612e60cae
bb51255ec929ae1fb34981b8b988769027ee49e68c0958a4a2a76b59a0dc1cff
51f44e31b0f3718a5d145a1f77fd79cbd7ff21fecf8bba3181fea019b508cfeb
73e19be4da76bb4e52cb82493c75690977fc3a5f589a9b47e834362545ef512a
bbd84d10f6a56bfeca23fd5d11d9e370fdfa91be73aa60c9d460b2671145c109
0ed328af77f2576071bfd543938fc01101daac01f216dc43bc091a8da4aff18d
f054f373cead893f868fd9b4acc24f751afefbb80cf961e305f97741f952a641
176476f9d924d83343a51a90ade097d12b7594dc5dbca1771c440047dfbe81eb
957a6aee2437a5c4d31372af2f6bceb29e1c7a49d650fe207cefc624bf6bca82
2e9126dfad03bdaf54f9b29ade42038c83f65ac7288376f45768901660f62d7b
2ab190542c3ec7b2b6e6d4bccce4c5d6a572f98c6bc89b014fea0c8fd6db6723

FortiGuard Labs Guidance

Due to the ease of disruption, damage to daily operations, potential impact to an organization's reputation, and the unwanted destruction or release of personally identifiable information (PII), etc., it is vital to keep all AV and IPS signatures up to date.

Since the majority of ransomware is delivered via phishing, organizations should consider leveraging Fortinet solutions designed to train users to understand and detect phishing threats:

The FortiPhish Phishing Simulation Service uses real-world simulations to help organizations test user awareness and vigilance to phishing threats and to train and reinforce proper practices when users encounter targeted phishing attacks.

Our FREE NSE training: NSE 1 – Information Security Awareness includes a module on internet threats designed to help end users learn how to identify and protect themselves from various types of phishing attacks and can be easily added to internal training programs.

Organizations will need to make foundational changes to the frequency, location, and security of their data backups to effectively deal with the evolving and rapidly expanding risk of ransomware. When coupled with digital supply chain compromise and a workforce telecommuting into the network, there is a real risk that attacks can come from anywhere. Cloud-based security solutions, such as SASE, to protect off-network devices; advanced endpoint security, such as EDR (endpoint detection and response) solutions that can disrupt malware mid-attack; and Zero Trust Access and network segmentation strategies that restrict access to applications and resources based on policy and context, should all be investigated to minimize risk and to reduce the impact of a successful ransomware attack.

As part of the industry's leading fully integrated Security Fabric, delivering native synergy and automation across your security ecosystem, Fortinet also provides an extensive portfolio of technology and human-based as-a-service offerings. These services are powered by our global FortiGuard team of seasoned cybersecurity experts.

Best Practices include Not Paying a Ransom

Organizations such as CISA, NCSC, the FBI, and HHS caution ransomware victims against paying a ransom partly because payment does not guarantee that files will be recovered. According to a U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) advisory, ransom payments may also embolden adversaries to target additional organizations, encourage other criminal actors to distribute ransomware, and/or fund illicit activities that could potentially be illegal. For organizations and individuals affected by ransomware, the FBI has a Ransomware Complaint page where victims can submit samples of ransomware activity via their Internet Crimes Complaint Center (IC3).

How Fortinet Can Help

FortiGuard Labs' Emergency Incident Response Service provides rapid and effective response when an incident is detected. And our Incident Readiness Subscription Service provides tools and guidance to help you better prepare for a cyber incident through readiness assessments, IR playbook development, and IR playbook testing (tabletop exercises).

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard AI-powered security services portfolio.