NETMANAGEIT

Intelligence Report

Frog4Shell — FritzFrog Botnet Adds One-Days to Its Arsenal

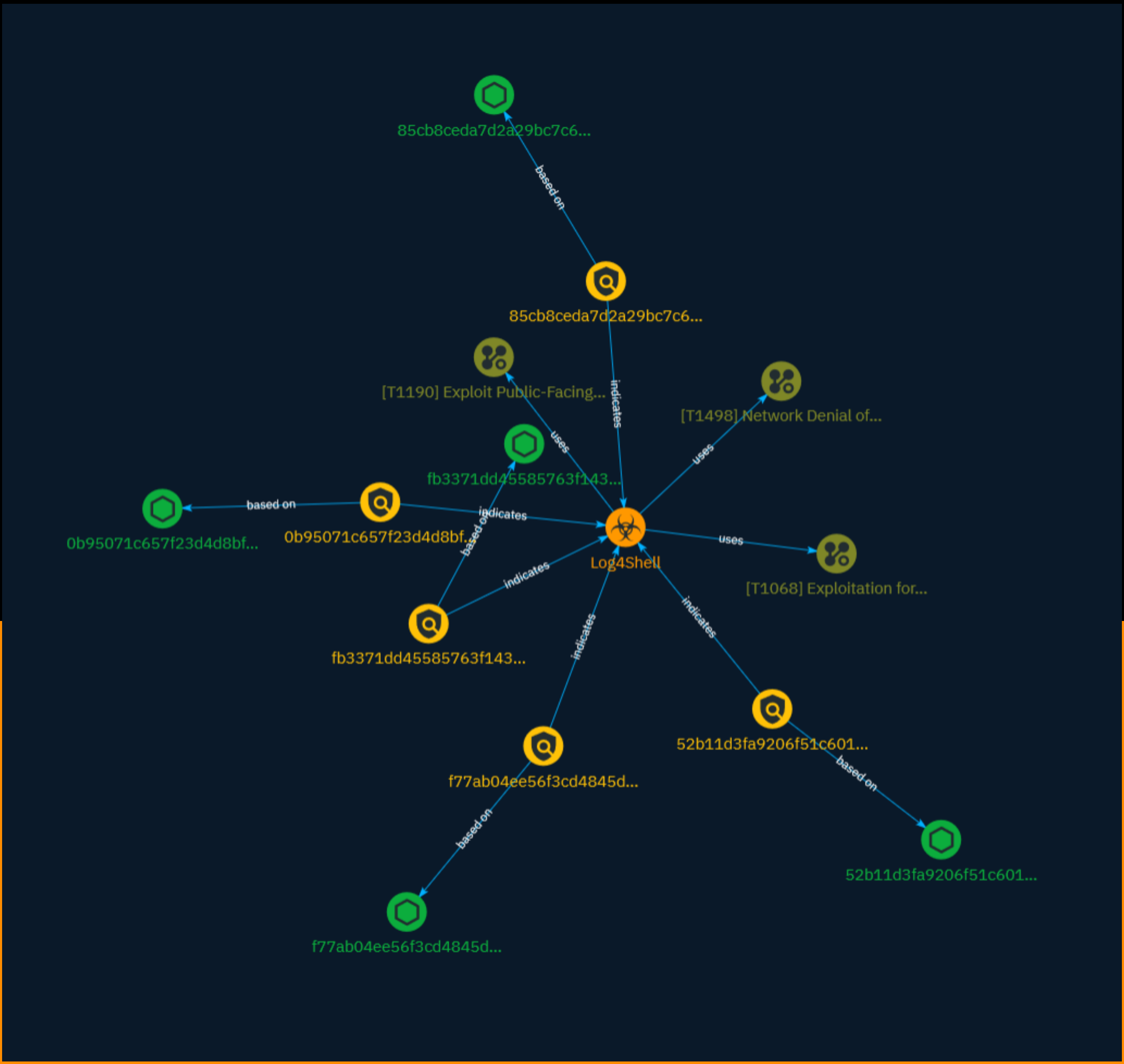

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The Akamai Security Intelligence Group (SIG) has uncovered details about a new variant of the FritzFrog botnet, which abuses the 2021 Log4Shell vulnerability. Over the years we have seen more than 20,000 FritzFrog attacks, and 1,500+ victims. The malware infects internet-facing servers by brute forcing weak SSH credentials. Newer variants now read several system files on compromised hosts to detect potential targets for this attack that have a high likelihood of being vulnerable. The malware also includes a module to exploit CVE-2021-4034, a privilege escalation in the polkit Linux component. This module enables the malware to run as root on vulnerable servers.

Confidence

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

15 / 100

Content

N/A

Indicator

Name

fb3371dd45585763f1436afb7d64c202864d89ee6cbb743efac9dbf1cefcc291

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fb3371dd45585763f1436afb7d64c202864d89ee6cbb743efac9dbf1cefcc291']

Name

f77ab04ee56f3cd4845d4a80c5817a7de4f0561d976d87563deab752363a765d

Description

is__elf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f77ab04ee56f3cd4845d4a80c5817a7de4f0561d976d87563deab752363a765d']

Name

85cb8ceda7d2a29bc7c6c96dd279c43559797a624fc15d44da53ca02379afe01

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '85cb8ceda7d2a29bc7c6c96dd279c43559797a624fc15d44da53ca02379afe01']

Name

52b11d3fa9206f51c601bd85cb480102fd938894b7274fac3d20915eb3af44f8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '52b11d3fa9206f51c601bd85cb480102fd938894b7274fac3d20915eb3af44f8']

Name

0b95071c657f23d4d8bfa39042ed8ad0a1c1bceb6b265c1237c12c4c0818c248

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'0b95071c657f23d4d8bfa39042ed8ad0a1c1bceb6b265c1237c12c4c0818c248']

Name

fb3371dd45585763f1436afb7d64c202864d89ee6cbb743efac9dbf1cefcc291

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'fb3371dd45585763f1436afb7d64c202864d89ee6cbb743efac9dbf1cefcc291']

Name

f77ab04ee56f3cd4845d4a80c5817a7de4f0561d976d87563deab752363a765d

Description

is__elf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'f77ab04ee56f3cd4845d4a80c5817a7de4f0561d976d87563deab752363a765d']

Name

85cb8ceda7d2a29bc7c6c96dd279c43559797a624fc15d44da53ca02379afe01

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'85cb8ceda7d2a29bc7c6c96dd279c43559797a624fc15d44da53ca02379afe01']

Name

52b11d3fa9206f51c601bd85cb480102fd938894b7274fac3d20915eb3af44f8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'52b11d3fa9206f51c601bd85cb480102fd938894b7274fac3d20915eb3af44f8']

Name

0b95071c657f23d4d8bfa39042ed8ad0a1c1bceb6b265c1237c12c4c0818c248

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0b95071c657f23d4d8bfa39042ed8ad0a1c1bceb6b265c1237c12c4c0818c248']

Malware

Name
Log4Shell

Name
Log4Shell

Attack-Pattern

Name
Network Denial of Service
ID
T1498
Description

Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth services rely on. Example resources include specific websites, email services, DNS, and web-based applications. Adversaries have been observed conducting network DoS attacks for political purposes(Citation: FireEye OpPoisonedHandover February 2016) and to support other malicious activities, including distraction(Citation: FSISAC FraudNetDoS September 2012), hacktivism, and extortion.(Citation: Symantec DDoS October 2014) A Network DoS will occur when the bandwidth capacity of the network connection to a system is exhausted due to the volume of malicious traffic directed at the resource or the network connections and network devices the resource relies on. For example, an adversary may send 10Gbps of traffic to a server that is hosted by a network with a 1Gbps connection to the internet. This traffic can be generated by a single system or multiple systems spread across the internet, which is commonly referred to as a distributed DoS (DDoS). To perform Network DoS attacks several aspects apply to multiple methods, including IP address spoofing, and botnets. Adversaries may use the original IP address of an attacking system, or spoof the source IP address to make the attack traffic more difficult to trace back to the attacking system or to enable reflection. This can increase the difficulty defenders have in defending against the attack by reducing or eliminating the effectiveness of filtering by the source address on network defense devices. For DoS attacks targeting the hosting system directly, see [Endpoint Denial of Service](https://attack.mitre.org/techniques/T1499).

Name

Exploitation for Privilege Escalation

ID

T1068

Description

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions. When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods. Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020) Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a compromised system via [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) or [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570).

Name

Exploit Public-Facing Application

ID

T1190

Description

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities.(Citation: OWASP Top 10)(Citation: CWE top 25)

Name

Network Denial of Service

ID

T1498

Description

Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth services rely on. Example resources include specific websites, email services, DNS, and web-based applications. Adversaries have been observed conducting network DoS attacks for political purposes(Citation: FireEye OpPoisonedHandover February 2016) and to support other malicious activities, including distraction(Citation: FSISAC FraudNetDoS September 2012), hacktivism, and extortion.(Citation: Symantec DDoS October 2014) A Network DoS will occur when the bandwidth capacity of the network connection to a system is exhausted due to the volume of malicious traffic directed at the resource or the network connections and network devices the resource relies on. For example, an adversary may send 10Gbps of traffic to a server that is hosted by a network with a 1Gbps connection to the internet. This traffic can be generated by a single system or multiple systems spread across the internet, which is commonly referred to as a distributed DoS (DDoS). To perform Network DoS attacks several aspects apply to multiple methods, including IP address spoofing, and botnets. Adversaries may use the original IP address of an attacking system, or spoof the source IP address to make the attack traffic more difficult to trace back to the attacking system or to enable reflection. This can increase the difficulty defenders have in defending against the attack by reducing or eliminating the effectiveness of filtering by the source address on network defense devices. For DoS attacks targeting the hosting system directly, see [Endpoint Denial of Service](https://attack.mitre.org/techniques/T1499).

Name

Exploitation for Privilege Escalation

ID

T1068

Description

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions. When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods. Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020) Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a compromised system via [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) or [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570).

Name

Exploit Public-Facing Application

ID

T1190

Description

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities.(Citation: OWASP Top 10)(Citation: CWE top 25)

StixFile

Value
fb3371dd45585763f1436afb7d64c202864d89ee6cbb743efac9dbf1cefcc291
f77ab04ee56f3cd4845d4a80c5817a7de4f0561d976d87563deab752363a765d
85cb8ceda7d2a29bc7c6c96dd279c43559797a624fc15d44da53ca02379afe01
52b11d3fa9206f51c601bd85cb480102fd938894b7274fac3d20915eb3af44f8
0b95071c657f23d4d8bfa39042ed8ad0a1c1bceb6b265c1237c12c4c0818c248
fb3371dd45585763f1436afb7d64c202864d89ee6cbb743efac9dbf1cefcc291
f77ab04ee56f3cd4845d4a80c5817a7de4f0561d976d87563deab752363a765d
85cb8ceda7d2a29bc7c6c96dd279c43559797a624fc15d44da53ca02379afe01
52b11d3fa9206f51c601bd85cb480102fd938894b7274fac3d20915eb3af44f8
0b95071c657f23d4d8bfa39042ed8ad0a1c1bceb6b265c1237c12c4c0818c248

External References

- https://otx.alienvault.com/pulse/65bcdb1d1e7f9b70bf1accaa