FORTINET

# OUTBREAK ALERTS

# ANNUAL REPORT

2022

# TABLE OF CONTENTS



# EXECUTIVE SUMMARY

In the year 2022, **FortiGuard IPS** and **FortiGuard AV/Sandbox** blocked three trillion and six trillion h vulnerabilities, malware and 0-day attacks. Those encompassed several thousand varieties of *Remo Cross-Site Scripting, Elevation of Privilege, Denial of Service, Trojans, Exploits.* FortiGuard Labs aler numerous critical threats throughout the year based on factors such as *proof-of-concept, attack vect attack, dependencies, and more.* This annual report covers:

- More than two-dozen Outbreak Alerts on vulnerabilities, targeted attacks, ransomware, and OT
- Highlights of older but commonly targeted CVEs, including classification of these vulnerabilities view of prevalence.
- Real-world data compiled by **FortiGuard** showing how these vulnerabilities are exploited in the
- Context around the entire attack surface to understand the components that can aid in protecti response.

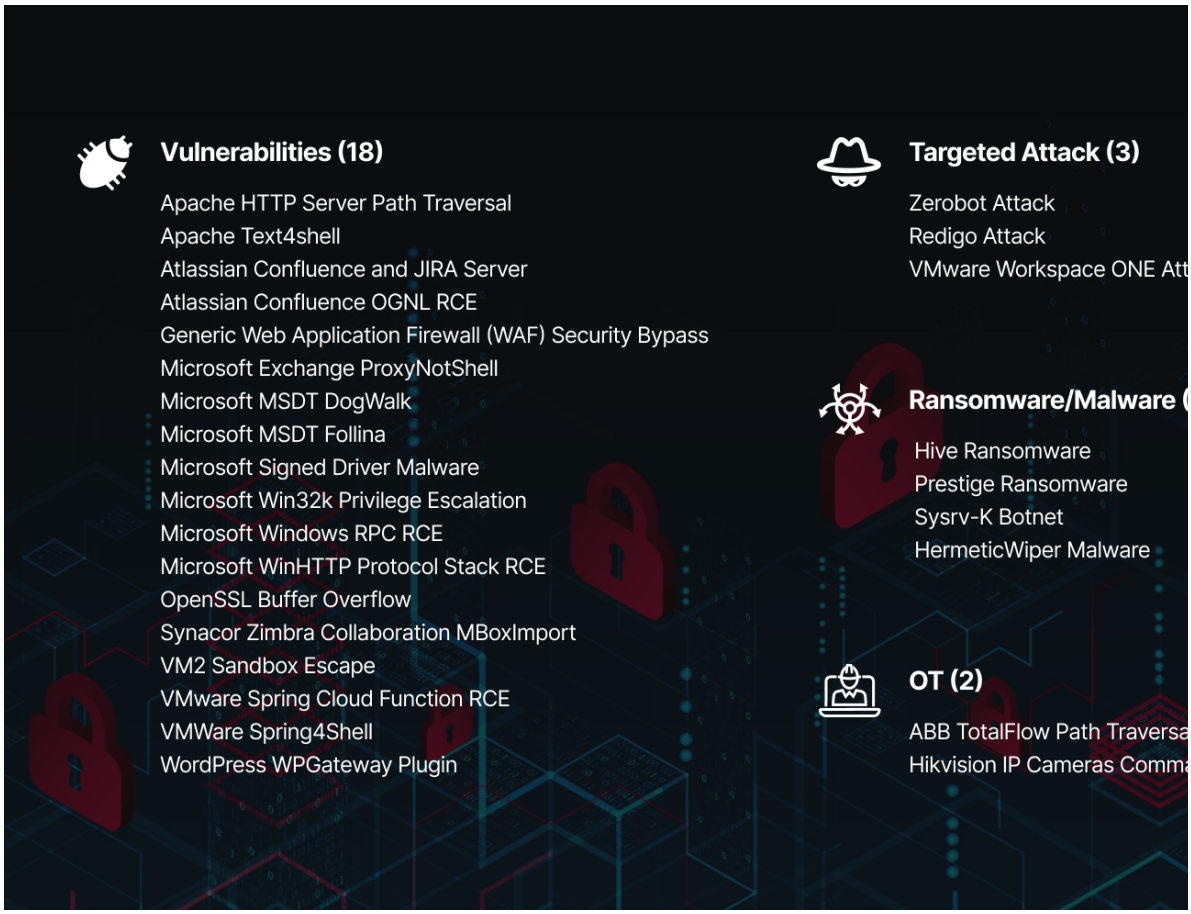



*Figure 1: FortiGuard Outbreak Alerts released in 2022*

## SIGNIFICANT OUTBREAKS IN 2O22

Given the enormous hits and varieties, let us focus on the significant ones:

### VMWare Spring4Shell (CVE-2022-22965)

With a few thousand daily average device attack hits, Spring4Shell is a sizable outbreak. Sprir is a popular Java lightweight open-source framework that allows simplification of the software cycle of any Java-based enterprise applications. Unpatched versions of the framework are eas to a remote code execution via insufficient validation of user-supplied inputs. Read the full Out

### Microsoft Exchange ProxyNotShell (CVE-2022-41040, CVE-2022-41082)

Microsoft Exchange has been on the top list of vulnerable applications with ten thousand daily attack hits. The vulnerability is due to insufficient sanitization when handling a malicious reque server is exploited, a remote attacker can disclose sensitive data or execute arbitrary code witl of the application. Read the full Outbreak Report.

### VMware Spring Cloud Function RCE (CVE-2022-22963)

Spring Framework is an open-source lightweight Java-based platform application developmen creating high-performing, easily testable code. Spring Cloud provides developer tools to build systems (e.g. configuration management, service discovery, etc). In Spring Cloud Function ver 3.1.6, and older versions, it is possible for an attacker to provide a specially crafted malicious e may result in remote code execution and access to local resources. Read the full Outbreak Re

### ABB TotalFlow Path Traversal (CVE-2022-0902)

Asea Brown Boveri (ABB), a Swiss industrial automation firm that develops flow computers, a purpose electronic instrument used by Energy sector manufacturers to interpret data and calcu gas flow rates. These devices are affected by a vulnerability that could allow hackers to cause prevent utilities from billing their customers. Read the full Outbreak Report.

### Hikvision IP Cameras Command Injection Vulnerability (CVE-2021-36260)

Hikvision is one of the leading providers of IoT sensor technologies such as IP cameras used energy, educational and military sectors. Our FortiGuard telemetry detected a daily average de thousand. An attacker can exploit this vulnerability to launch a command injection attack by se messages with malicious commands. . Read the full Outbreak Report.

### Hive Ransomware

Hive ransomware was first observed in June 2021. It has grown into one of the most prevalent the ransomware as a service (RaaS) ecosystem. The RaaS model has developers creating, m updating the malware, and affiliates conducting the ransomware attacks. According to FBI info Hive gang has received up to $100+ million in ransom payments from more than a thousand v the full Outbreak Report.

### Zerobot Attack

Zerobot is a Go-based botnet that spreads primarily through IoT and web application vulnerab According to the FortiGuard Labs research, the most recent distribution of Zerobot introduces including DDoS attack option and ability to exploit Apache vulnerabilities. It contains modules f replication, attacks for different protocols, and self-propagation. Read the full Outbreak Report

## VULNERABILITY PROFILE SUMMARY FOR 2022

For the top vulnerability profile, the code execution was the most prevalent. Attackers focus on remot vulnerabilities because of the high impact of successful exploitation. Many other vulnerabilities in the associated to websites such as accessing restricted directories, revealing sensitive information and u validation.

Some vulnerabilities were detected by more than 50,000 unique devices indicating widespread use b

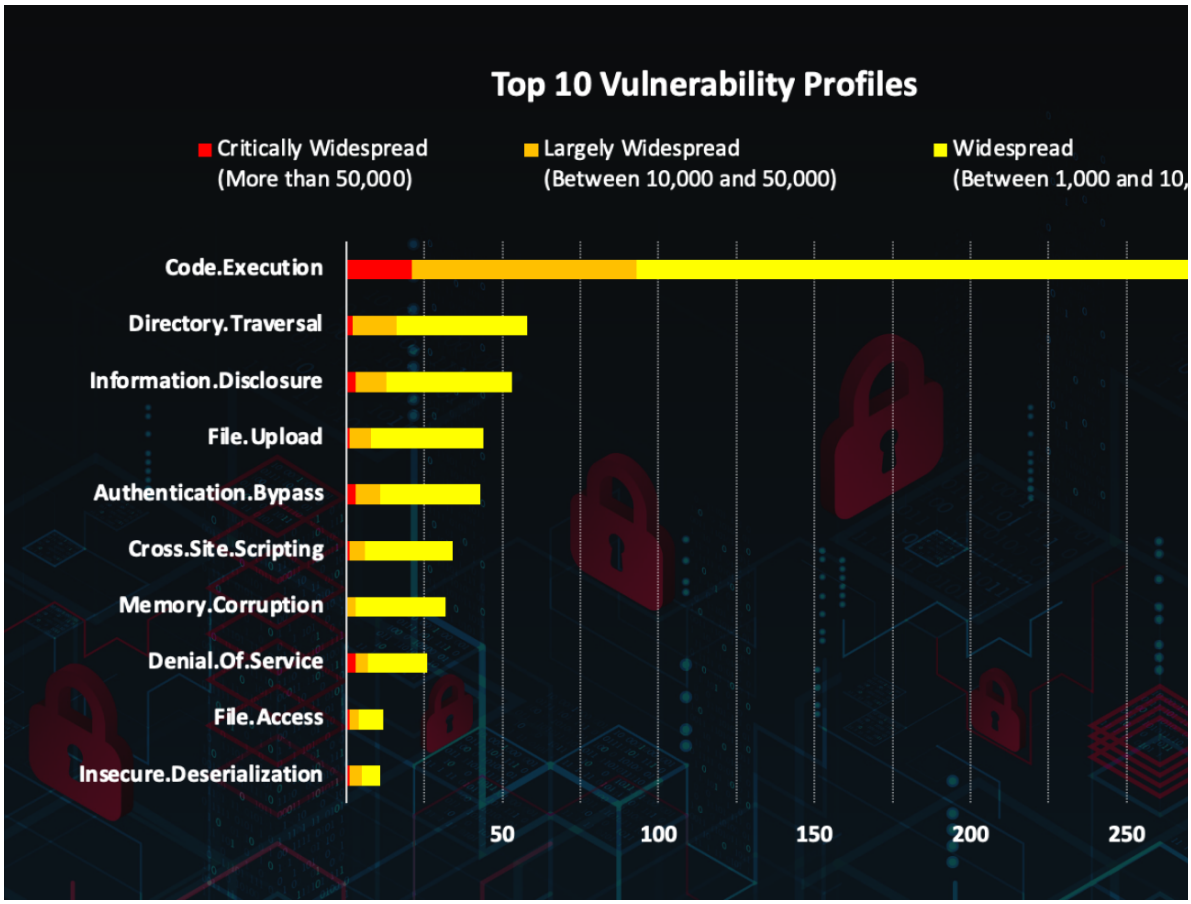



*Figure 2: Active vulnerability count detected by at least 1,000 unique devices in a month.*

Let's review the notable ones:

### Apache.Log4j.Error.Log.Remote.Code.Execution

The Log4j2 is a Java-based logging utility that is part of the Apache Logging Services project. vast number of companies worldwide, enabling logging in a wide set of popular applications. T vulnerability could allow a remote attacker to execute arbitrary code on the affected system. R Threat Encyclopedia entry for more info.

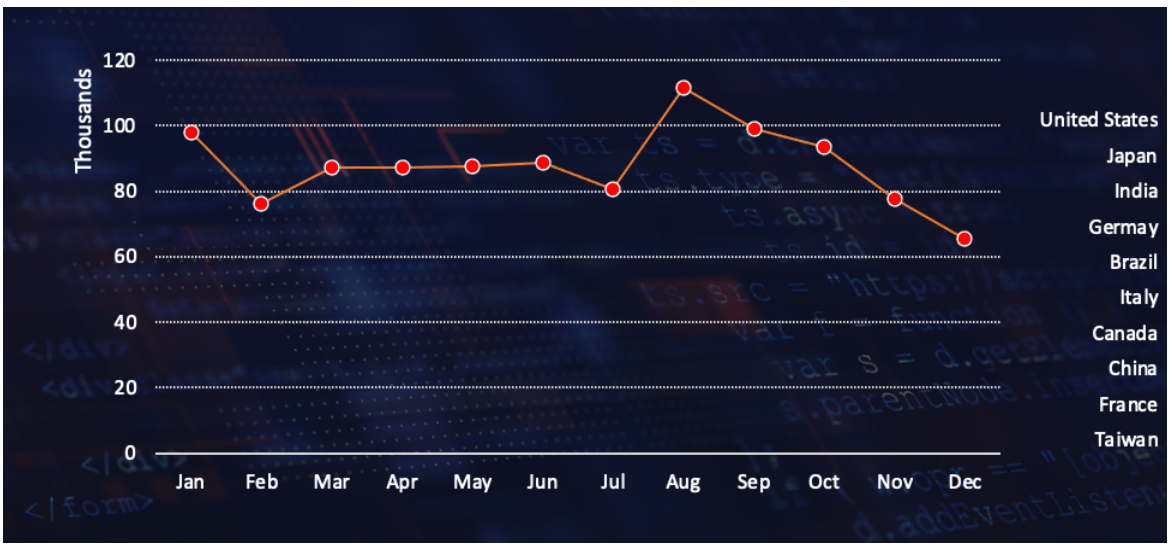



*Figure 3: Device hits for Apache.Log4j.Error.Log.Remote.Code.Execution and the locations of the attac*

### MS.Windows.CVE-2020-1381.Privilege.Elevation

This vulnerability is a privilege escalation vulnerability in Microsoft Windows, exploitable using crafted file. It has been publicly disclosed for more than two years and it remains to be in the to the attackers since there are hundreds of vulnerable devices and it can leverage their privilege Read the full IPS Threat and Endpoint Encyclopedia entries for more info.

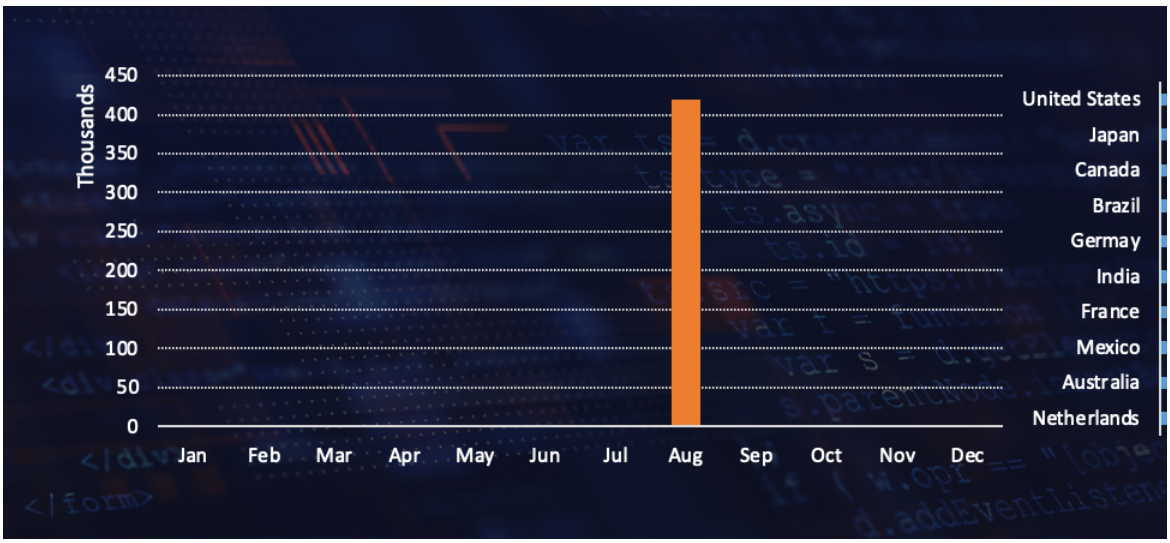



*Figure 4: Device hits for MS.Windows.CVE-2020-1381.Privilege.Elevation and the locations of the attac*

## Apache.HTTP.Server.cgi-bin.Path.Traversal

This indicates an attack attempt to exploit a path traversal vulnerability in Apache HTTP Serve vulnerability is due to a path normalization error. Successful exploitation can lead to informatio Read the full Threat Encyclopedia entry for more info.

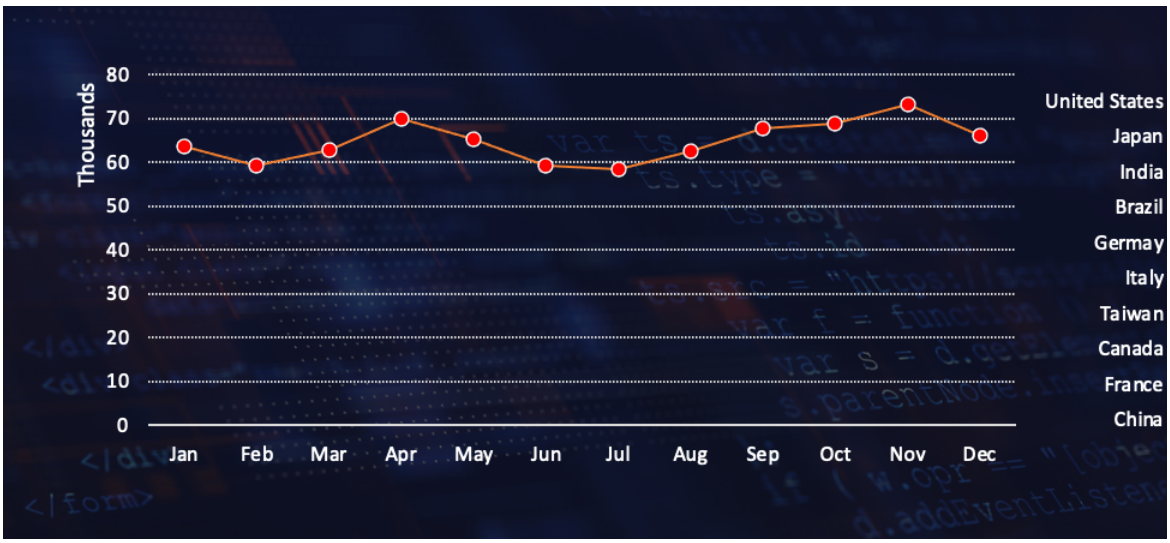
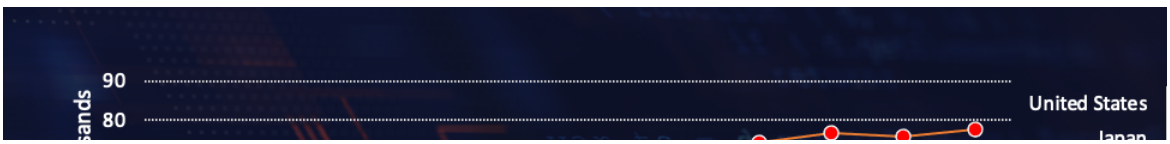



*Figure 5: Device hits for Apache.HTTP.Server.cgi-bin.Path.Traversal and the locations of the attacks*

## Linux.Kernel.TCP.SACK.Panic.DoS

This vulnerability is due to an error in the Linux kernel when it handles specially crafted TCP p segment size. A remote attacker may be able to exploit this to cause a denial of service conditi targeted system. Read the full Threat Encyclopedia entry for more info.



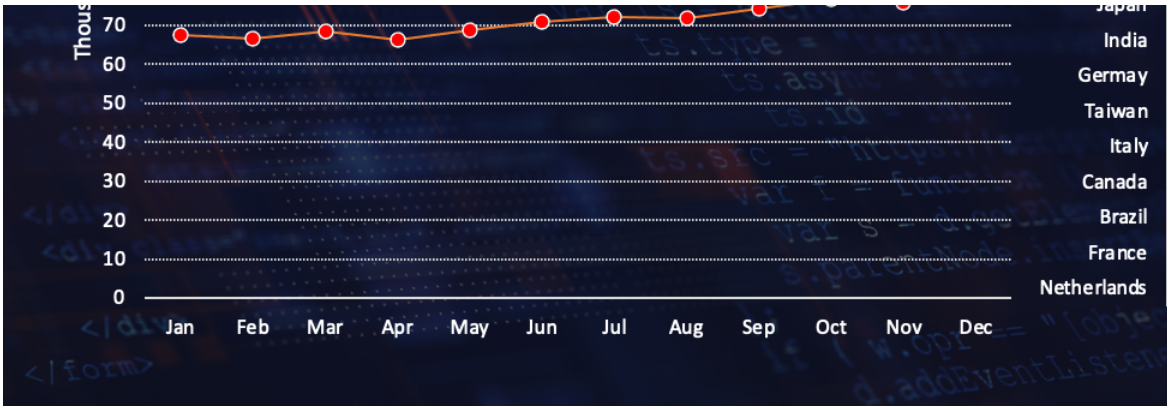



*Figure 6: Device hits for Linux.Kernel.TCP.SACK.Panic.DoS and the locations of the attacks bloc*

## MALWARE PROFILE SUMMARY FOR 2022

FortiGuard Labs observed an average of over 500 million total malware detections per month in 2022 September, there was increased activity due to regionally-focused MSIL/Packer attacks. In addition, million monthly 0-day attacks were detected by FortiSandbox. Microsoft Windows executable file type common vehicle for malware attacks followed by Microsoft Office file type.

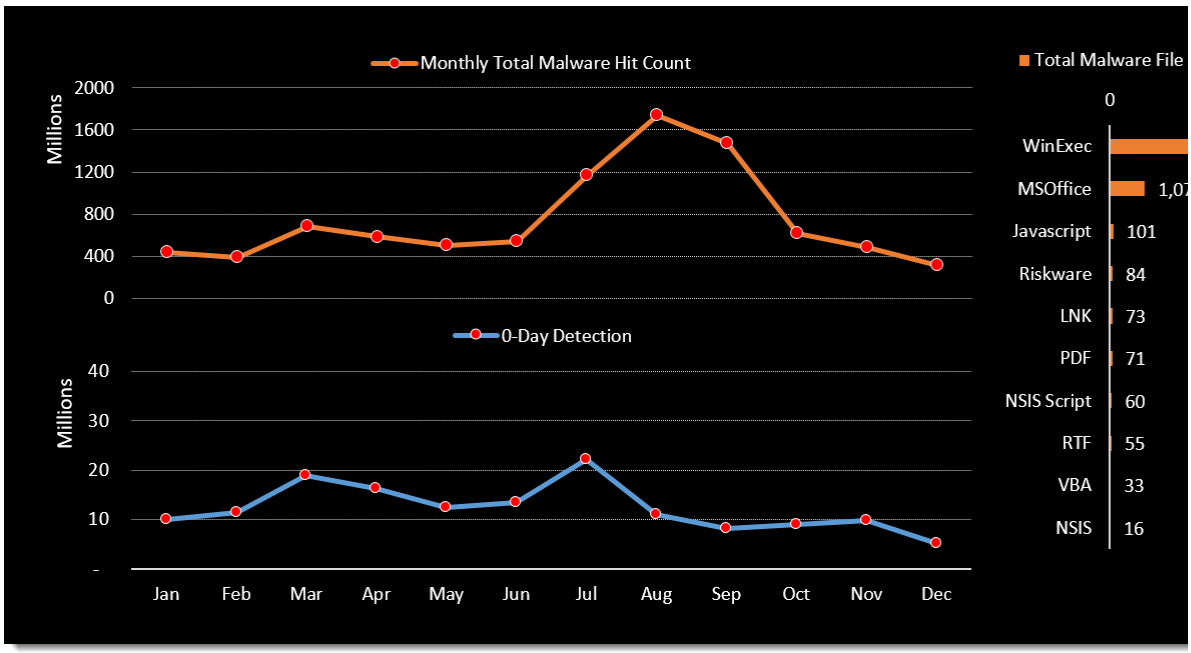



*Figure 7: Overall Monthly Malware hit count, file type and country distribution.*

Let's review the notable ones:

### MSIL/Packer

The MSIL/Packer.VWH!tr and MSIL/Packer.VZX!tr were regionally widespread in Columbia wit 2.5 billion total detections. This malware used a Windows DLL program based on .NET and pa multiple encryptions. Read the full Threat Encyclopedia entry for more info.


*Figure 8: Monthly detection hit count of MSIL/Packer.*

## MSExcel/Exploits

Microsoft Excel exploits remained popular with more than 500 million detection hit count. The r
vulnerabilities targeted were CVE-2017-11882 and CVE-2018-0798, which both are 5. Given it
presence and year round, many endpoints are presumed to be still vulnerable. The malware w
stack buffer overflow vulnerability to run malicious shellcode which in turn will allow the malwa
download the next malicious payload. For more info, here are the MSOffice/CVE_2017_11882
MSExcel/CVE_2018_0798.BOR!exploit.


*Figure 9: Monthly detection hit count of malware targeting CVE-2017-11882.*


*Figure 10: Monthly detection hit count of malware targeting CVE-2018-0798.*

## CONCLUSION

Attacks on open source and common vulnerabilities accelerated throughout 2022, becoming more w
for all types of organization. Targeted attacks are becoming easier as attackers gain awareness of th
industry, plus commonly used devices (IoT), or other malpractices adopted during the work-from-any
Zero trust of endpoints combined with automated insights to attacks and industry trends are keys for

## ABOUT FORTIGUARD OUTBREAK ALERTS

Given the volume of active threats, evolving methods for exploiting systems and increasing damage t
operations, today's SOC teams require automation and dynamic services to succeed.
FortiGuard Labs Outbreak Alerts provide a unique analysis of the threat landscape throughout the tec
FortiGuard Services provide solutions to cover the complete attack surfaces, identify outbreaks and a
mitigate impacts and investigate suspected compromises.

Learn more about FortiGuard Outbreak Alerts