



FORTINET

FortiGuard Labs Threat Landscape Highlights

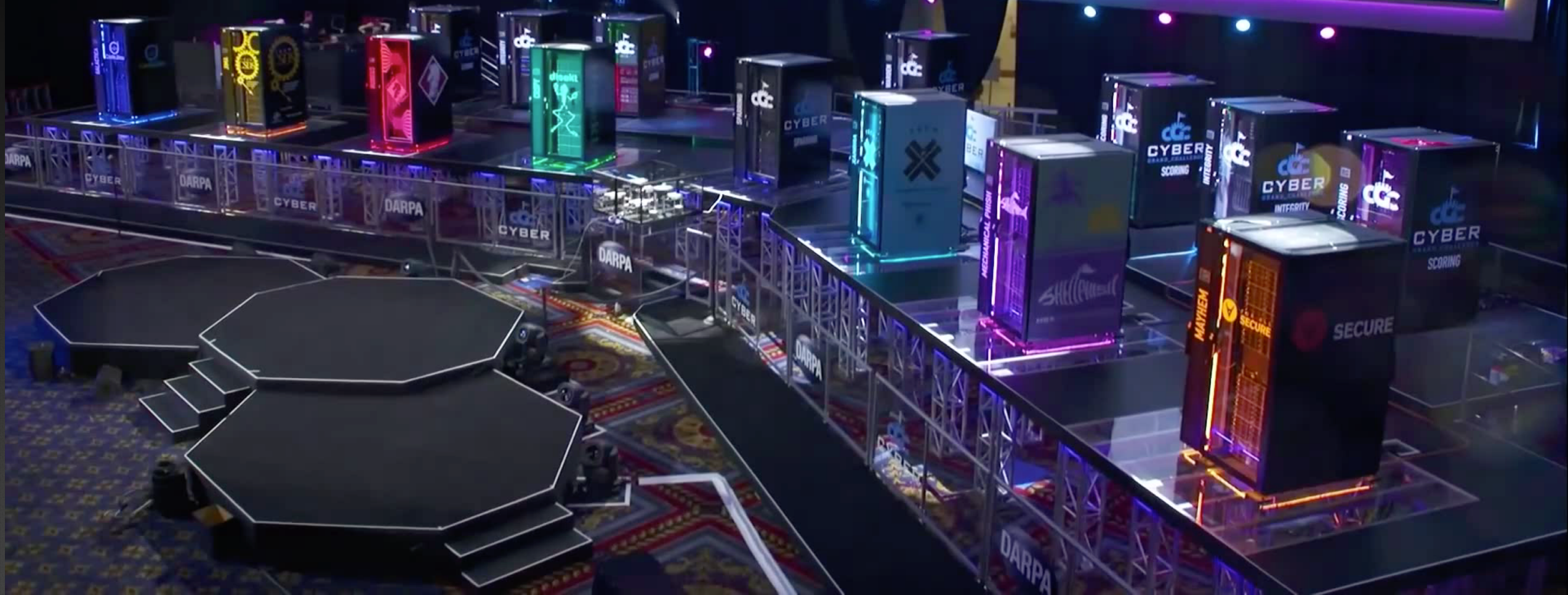
MNSEC 2018

2018 Threat Landscape Predictions

FortiGuard Labs

PREDICTION:

**NEXT-GEN
MORPHIC
MALWARE**



PREDICTION:

**CRITICAL
INFRASTRUCTURE
TO THE FOREFRONT**

[HACKING]
AMERICA

OFFICIALS: HUNDREDS OF
U.S. ELECTRIC PLANTS HACKED

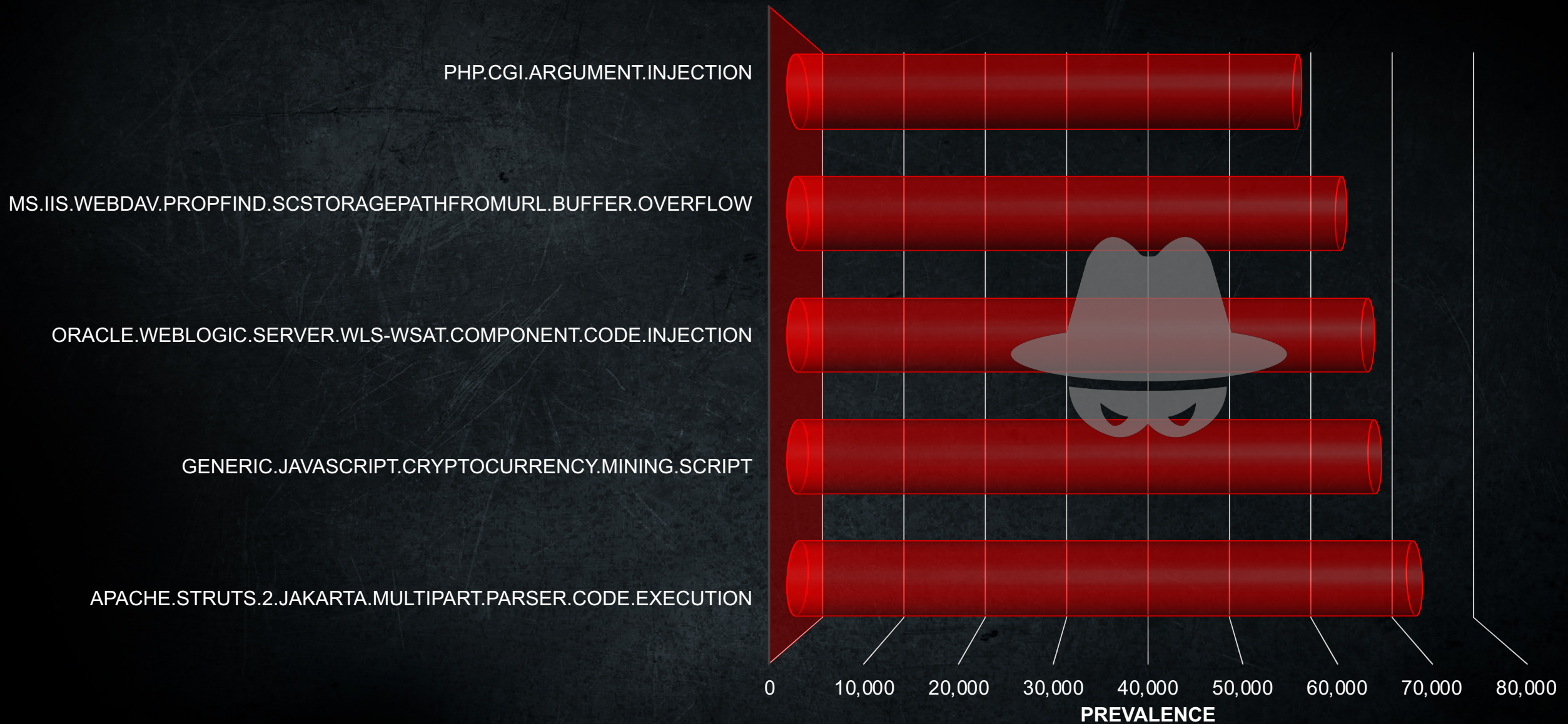
 **CNBC**

A nighttime aerial view of a city with illuminated buildings and streets. The lights create a vibrant, colorful scene with various shades of yellow, white, and blue. The city is densely packed with structures, and the overall atmosphere is one of a bustling urban environment at night.

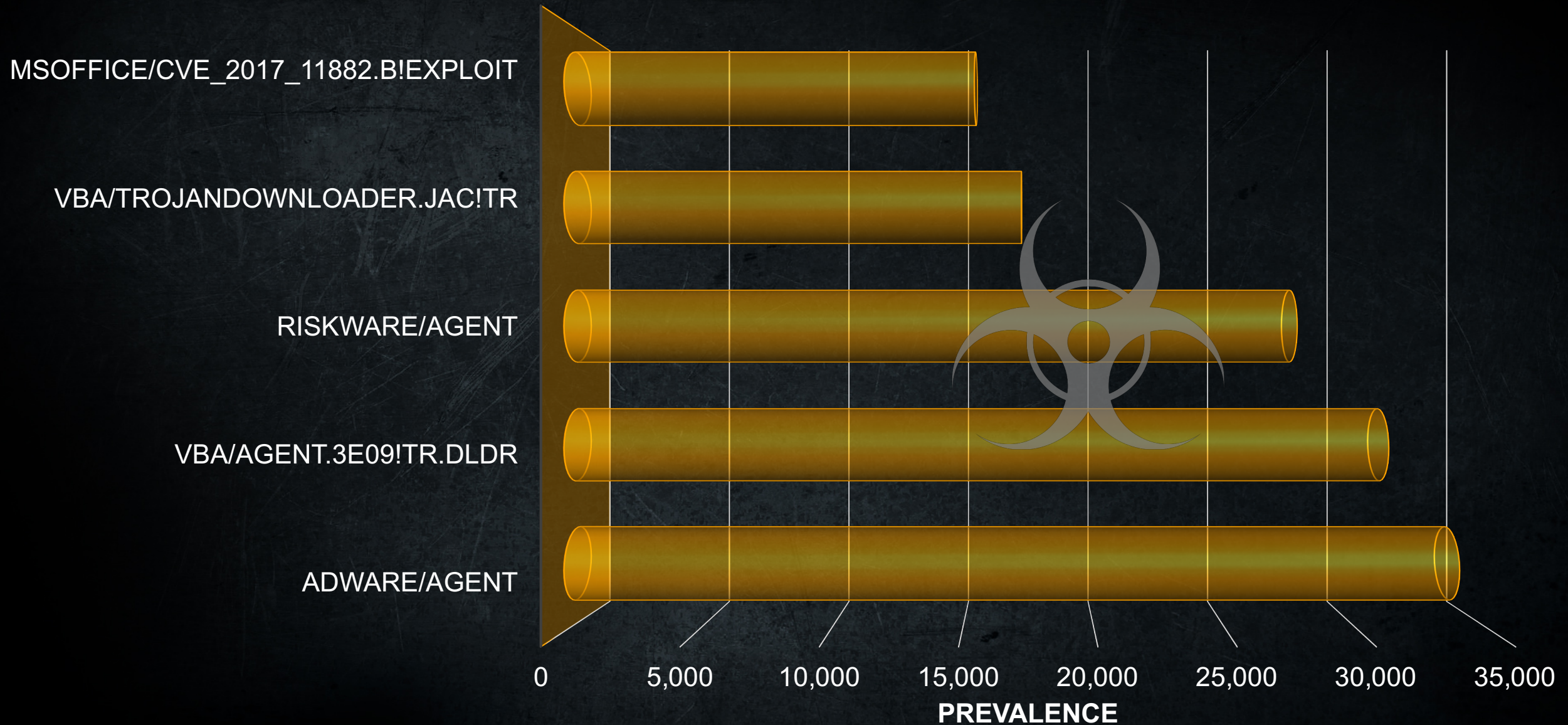
FortiGuard Labs Threat Telemetry

Global and Mongolia – 2018 (Thus Far)

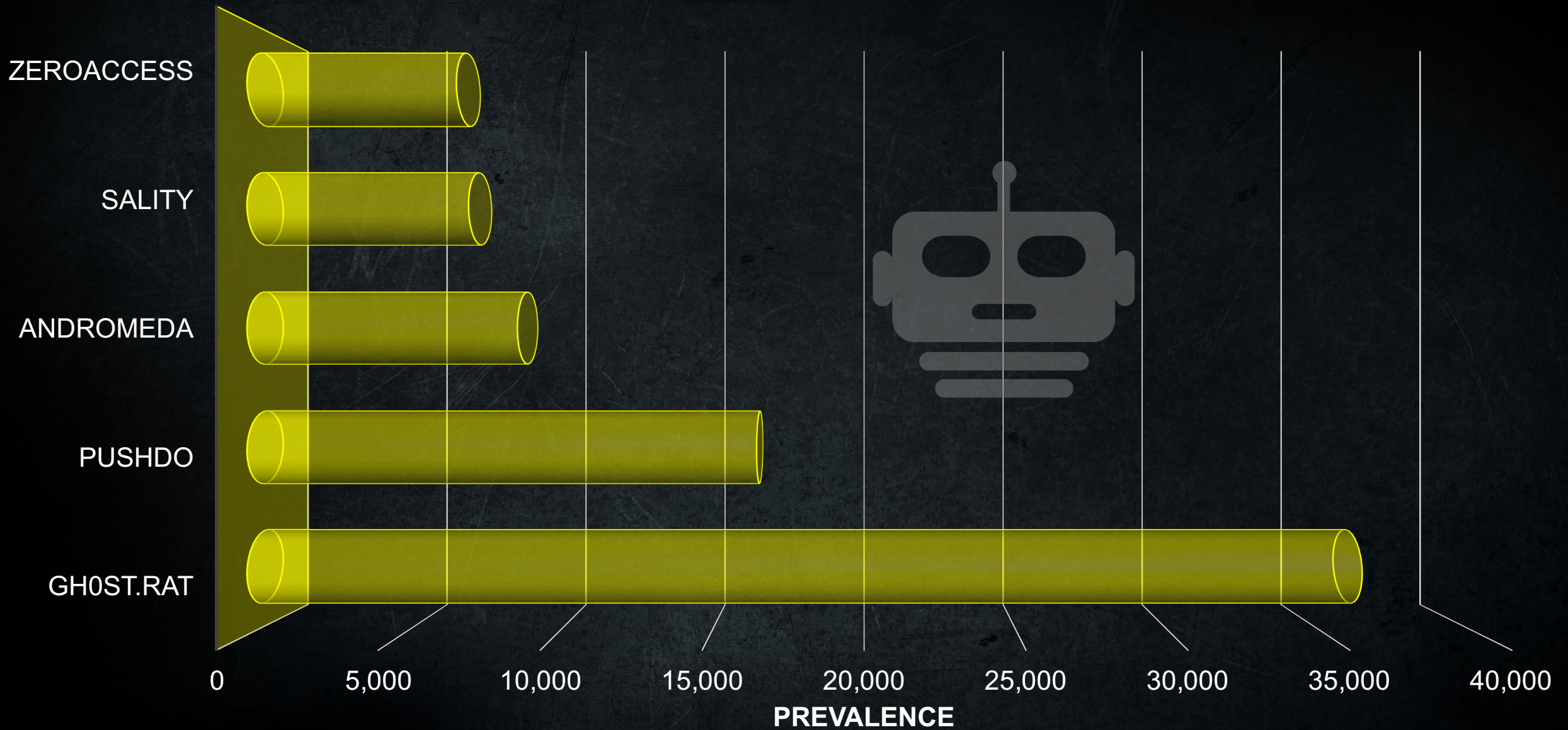
Top 5 Prevalent Attacks – Global



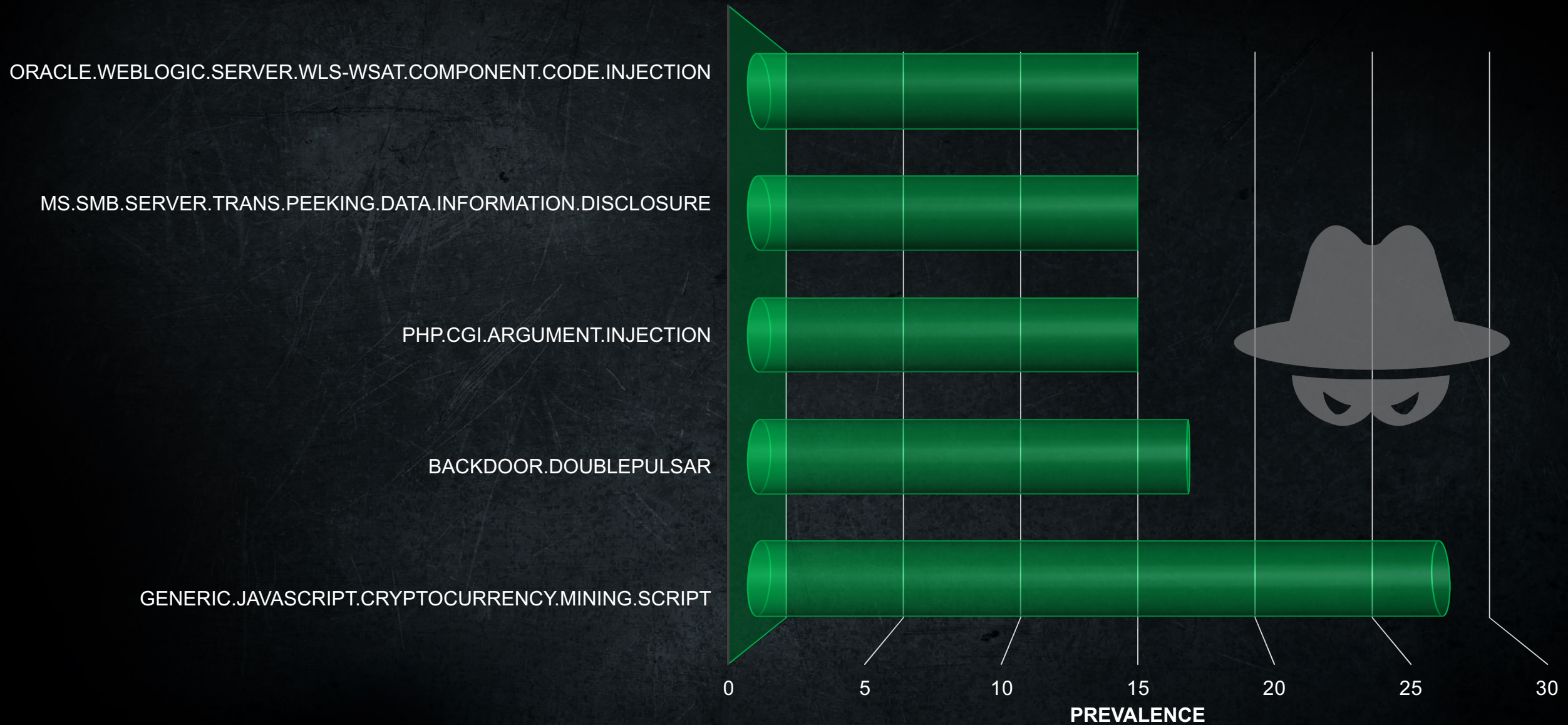
Top 5 Prevalent Malware – Global



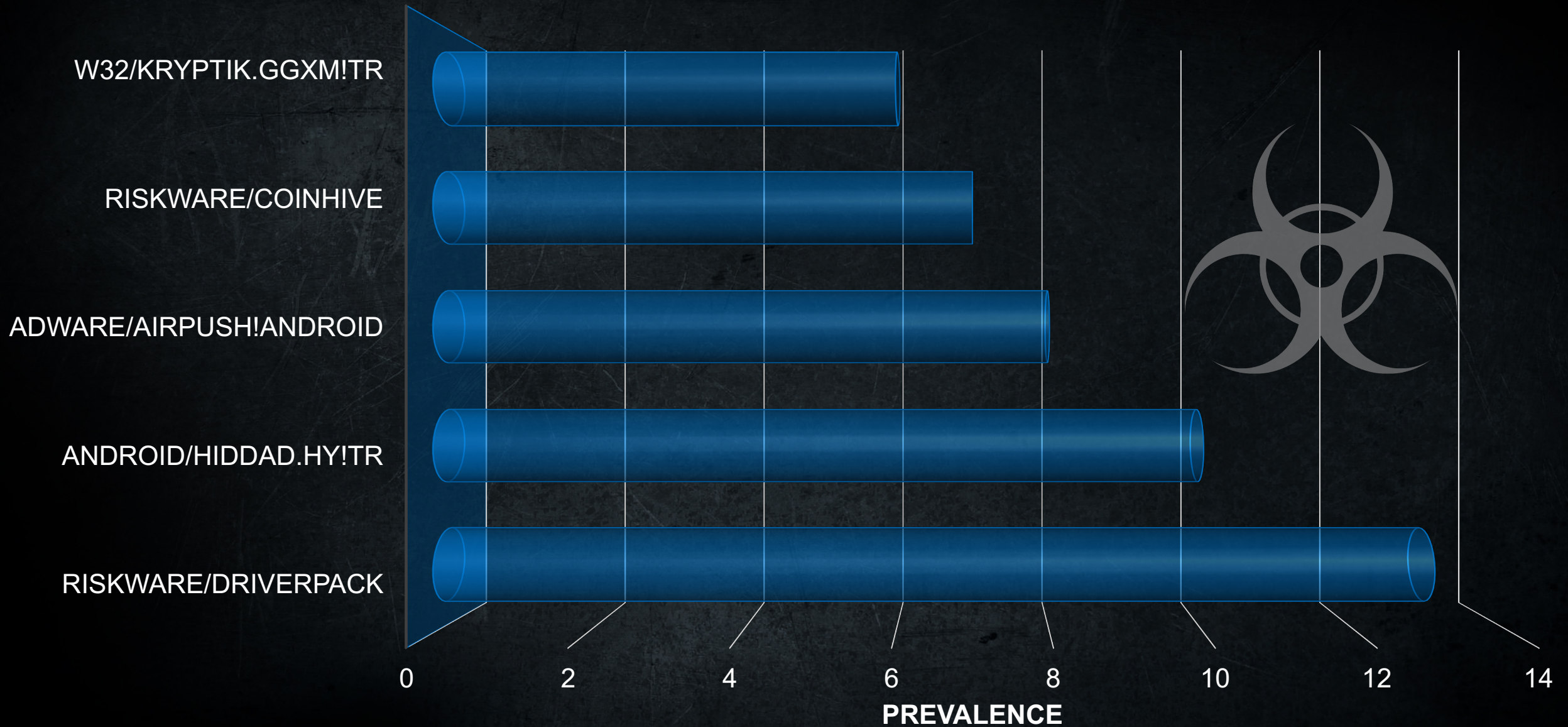
Top 5 Prevalent Botnets – Global



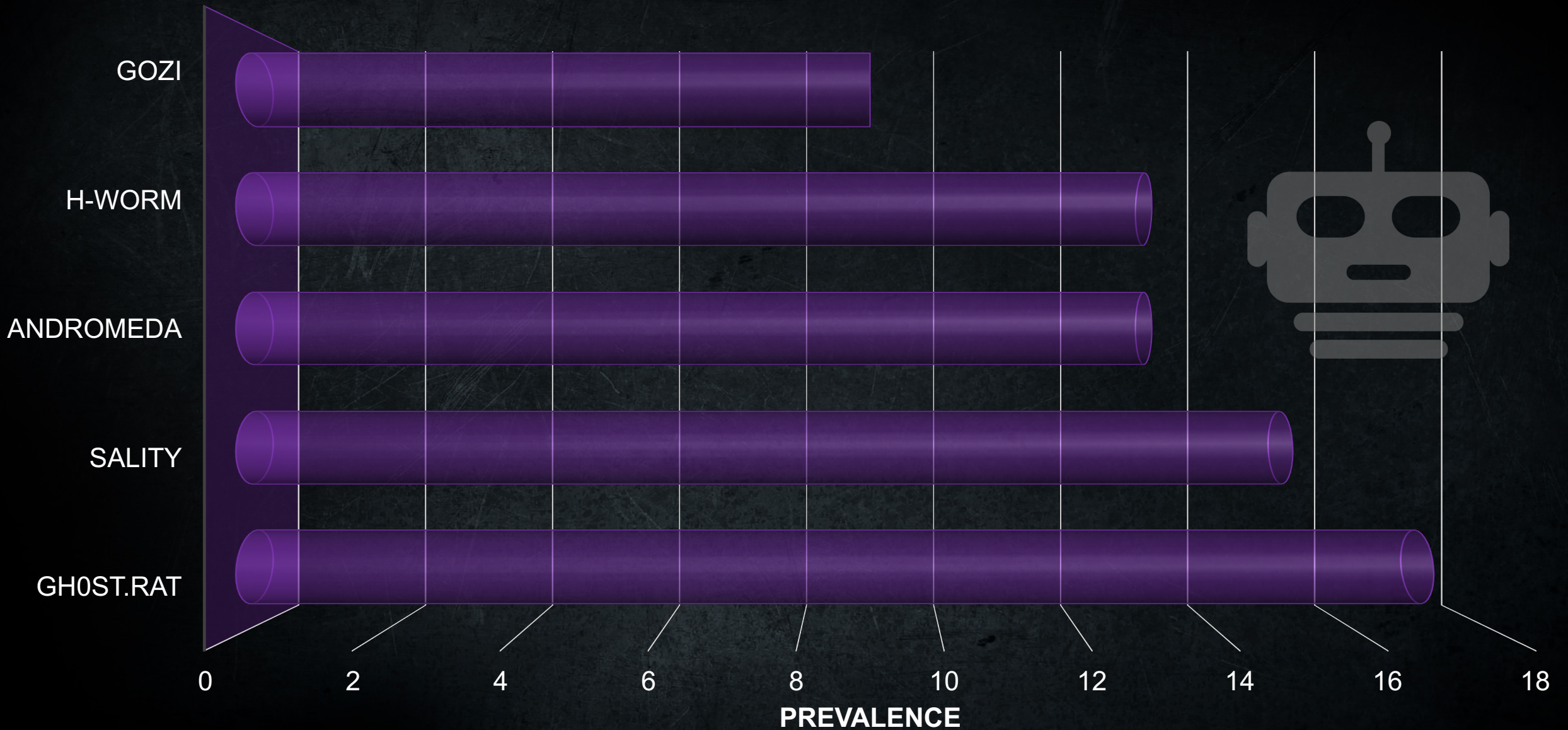
Top 5 Prevalent Attacks – Mongolia



Top 5 Prevalent Malware – Mongolia



Top 5 Prevalent Botnets – Mongolia





Quarterly Threat Landscape Report

Q2 2018

CAN YOU PATCH 'EM ALL?

KNOWN VULNERABILITIES (CVEs)

103,786



**IT'S KEY TO USE THREAT INTELLIGENCE
TO PRIORITIZE PATCHING**

96%

SAW SEVERE
EXPLOITS



ONLY **5.7%**
OF KNOWN VULNERABILITIES
WERE TARGETED

CVE-2017-5638 – Apache Struts 2 RCE

The image shows a desktop environment with two windows. The left window is a Mozilla Firefox browser displaying the Struts2 Showcase page. The address bar shows the URL `10.178.178.3:8080/struts2-showcase/index.action`. The page content includes a "Welcome!" heading, a paragraph about the showcase, and a "View Sources" button. The right window is a Terminal window running Metasploit (msf). The terminal prompt is `msf exploit(multi/http/struts2_content_type_ognl) >`, and the cursor is positioned at the end of the line.

Applications ▾ Places ▾ Terminal ▾ Fri 16:15

Struts2 Showcase - Mozilla Firefox

Struts2 Showcase

Welcome!

The [Struts Showcase](#) demonstrates a variety of use cases and tag usages. Essentially, the application exercises various framework features in isolation. The Showcase is not meant as a "best practices" example.

For more "by example" solutions, see the [Struts Cookbook >>](#) pages.

[View Sources](#)

Copyright © 2003-2018 [The Apache Software Foundation](#). 2018/07/06 04:05:45
Powered by **Struts**

Terminal

```
File Edit View Search Terminal Help
msf exploit(multi/http/struts2_content_type_ognl) >
```


AGILE DEVELOPMENT IS ON THE LOOSE



AGILE DEVELOPMENT
USED IN CONJUNCTION
WITH POLYMORPHISM



THIS MALWARE IS
MORE DIFFICULT
TO DETECT



A NEW RANSOMWARE SECURITY
TOOL WAS NEGATED
WITHIN 48 HOURS OF RELEASE

GandCrab 2.1 Ransomware on the Rise with New Spam Campaign

By Jasper Manuel, Joie Salvio, and Rommel Joven | April 25, 2018

Over the past few days, FortiGuard Labs has been observing a surge in an email spam campaign. This article provides a basic overview of this malicious campaign, and points to the source of the malware.

Spam Campaign

The image below is a screenshot from our KTIS (Kadena Threat Intelligence System) showing a GandCrab v2.1 sample being delivered as a payload.

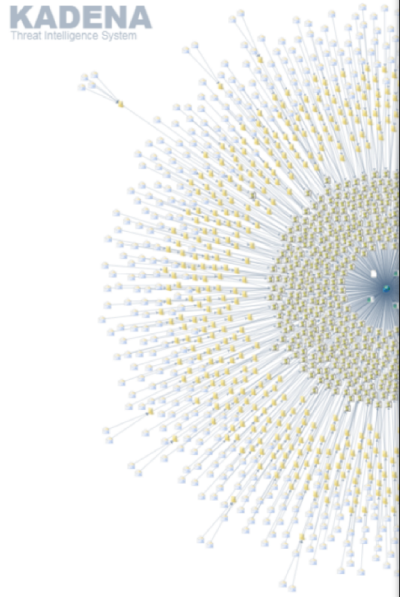


Fig.1 KTIS visualization of the spam

GandCrab V3 Accidentally Changes Systems with New 'Change Wallpaper' Feature

By Joie Salvio | May 04, 2018



GandCrab is one of the most talked about ransomware families this year primarily due to its increasing distribution. At the end of last month, FortiGuard Labs discovered a new spam wave from the same campaign as GandCrab v3.

In this new version, following in the footsteps of past infamous ransomware families such as Locky and Sage, this latest version now also changes the wallpapers of its victims. However, when we analyzed this new feature we found a bug that can be detrimental to its goals, as well as more frustrating to its unfortunate victims.

New Spam Wave, Same Old Tricks

The attack chain is practically the same as the one discussed in our previous article. Only this time, it uses Visual Basic Scripts as downloaders instead of Java Scripts.

GandCrab V4.0 Analysis: New Shell, Same Old Menace

By Joie Salvio | July 09, 2018

The new GandCrab v4.0 was seen just a few days ago targeting users. Malicious pages are currently being injected into legitimate websites.

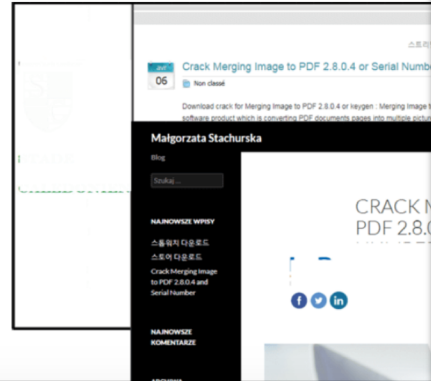
It has been over two months since GandCrab has undergone a major update. Its major purposes are practically the same. While some of the changes are new, the wallpaper change that had been added in the previous version, however, is the switch from using RSA-2048 to the much faster Petya ransomware in the past. Furthermore, it has done away with the ability to encrypt users that are not connected to the Internet.

Note: Thanks to David Maciejak, Director of FortiGuard Research Team, for the information.

Note: Read previous research on this topic.

Compromised Websites Serve GandCrab V4.0

The malware was reportedly seen being distributed through compromised websites. WordPress is a favorite target of exploitation. In fact, for this latest release, a few of which are shown in the figure below.



GandCrab v4.1 Ransomware and the Speculated SMB Exploit Spreader

By Joie Salvio | July 12, 2018

Only two days after the release of GandCrab 4.0, FortiGuard Labs found a newer version (v4.1) being distributed using the same method, which is through compromised websites disguised as download sites for cracked applications.

With this new version, GandCrab has added a network communication tactic that was not observed in the previous version. In addition, we will be sharing our analysis of currently circulating reports concerning an alleged "SMB exploit spreader" threat.

Network Communication



Figure 1 Malware sends info to list of compromised websites

This new version of the GandCrab malware contains an unusually long hard-coded list of compromised websites that it connects to. In one binary, the number of these websites can go up to almost a thousand unique hosts.

To generate the full URL for each host, a pseudo-random algorithm is used to choose from sets of pre-defined words. The final URL is in the following format (e.g. `www.{host}.com/data/tmp/sokakeme.jpg`):

`http://{host}/{word1}/{word2}/{fname}.{extension}`

DRUPAL EXPLOIT LED TO CRYPTOJACKING

**IOT DEVICES
SERVE AS A BASE
FOR CRYPTOJACKING**



“DRUPALGEDDON 2”
DETECTIONS SHOWED
**A THOUSAND-FOLD
INCREASE OVER 24 HOURS**



ESPECIALLY POPULAR
CRYPTOJACKING TARGETS ARE
**MEDIA DEVICES DUE TO
POWERFUL GPUS**

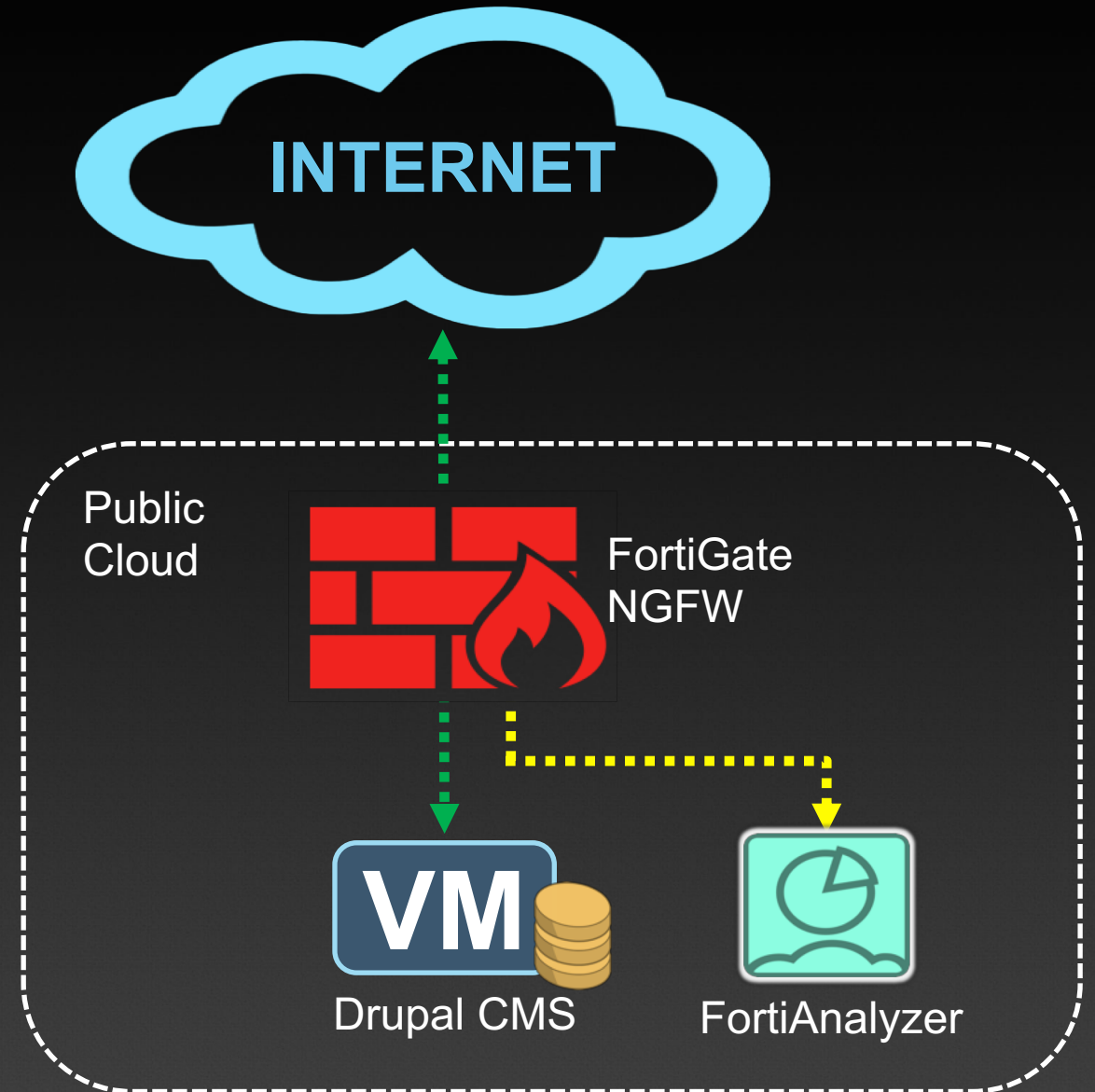


Web Honeypot

Drupal CMS deployed on a Linux Instance

FortiGate NGFW in **Monitoring Mode**

FortiAnalyzer for Centralized Reporting



CVE-2018-7600 - Drupal RCE

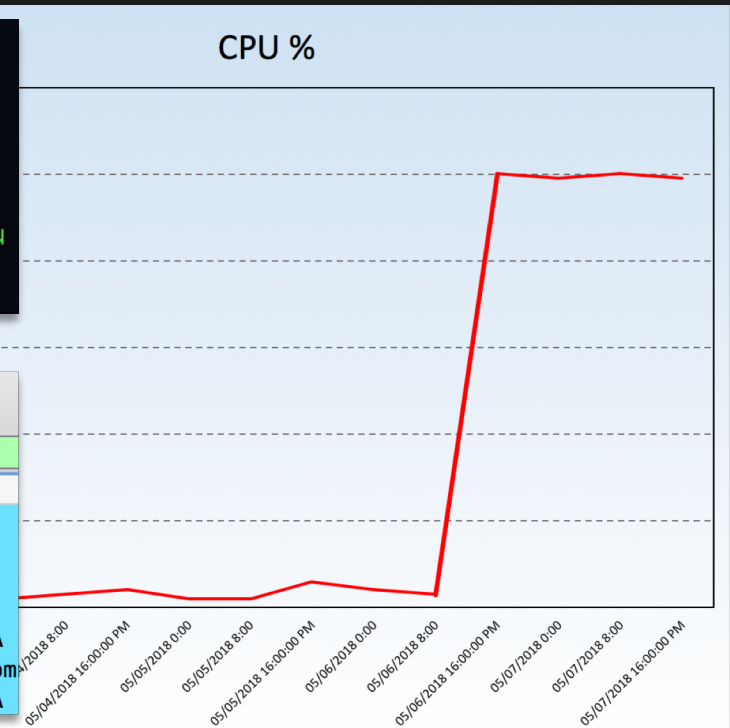
The image shows a dual-pane view of a Kali Linux system. The left pane is a Firefox ESR browser window displaying the homepage of 'AWESOME ONLINE SUPERMARKET' at IP 10.178.178.4. The page features a blue header with the Drupal logo and the text 'AWESOME ONLINE SUPERMARKET'. Below the header is a 'Home' button and a main content area with the heading 'Welcome to AWESOME ONLINE SUPERMARKET' and a message: 'No front page content has been created yet. Follow the [User Guide](#) to start building your site.' There is also a search bar with the placeholder text 'Search'.

The right pane is a terminal window titled 'root@nix: ~/Downloads/Drupalgeddon2'. The terminal shows the prompt 'root@nix:~/Downloads/Drupalgeddon2#' with a cursor, indicating that the user is in the directory where the exploit script is located.

Server Side Cryptojacking

#	Threat	Category	Threat Level
1	Drupal.Core.Form.Rendering.Component.Remote.Code.Execution	IPS	Critical
2	Oracle.WebLogic.Server.wls-wsat.Component.Code.Injection	IPS	Critical
3	MS.IIS.WebDAV.PROPFIND.ScStoragePathFromUrl.Buffer.Overflow	IPS: CVE-2017-7269	Critical
4	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	IPS	Critical
5	Linksys.Routers.Administrative.Console.Authentication.Bypass	IPS	High

```
@drupalserver:/var/log/apache2# netstat -ntap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1013/sshd
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      3736/mysqld
tcp        0      0 *:*:56587               0.0.0.0:*               ESTABLISHED 9387/
tcp        0      0 *:*:22                   0.0.0.0:*               ESTABLISHED 13686/sshd: ubuntu
tcp6       0      0 :::22                   :::*                     LISTEN      1013/sshd
tcp6       0      0 :::80                   :::*                     LISTEN      8009/apache2
```



No.	Time	SrcPort	DstPort	Length	Protocol	Info
3006	2018-05-06 19:44:14.340030	37380	53	76	DNS	Standard query 0x7969 A pool.minexmr.com
3007	2018-05-06 19:44:14.340070	37380	53	76	DNS	Standard query 0x7969 A pool.minexmr.com
3008	2018-05-06 19:44:14.340096	37380	53	76	DNS	Standard query 0x80a1 AAAA pool.minexmr.com
3009	2018-05-06 19:44:14.340101	37380	53	76	DNS	Standard query 0x80a1 AAAA pool.minexmr.com
3010	2018-05-06 19:44:14.344263	53	37380	380	DNS	Standard query response 0x7969 A pool.minexmr.com A
3011	2018-05-06 19:44:14.345626	53	37380	136	DNS	Standard query response 0x80a1 AAAA pool.minexmr.com
3013	2018-05-06 19:44:14.347338	53	37380	380	DNS	Standard query response 0x7969 A pool.minexmr.com A

Client Side Browser Based Cryptojacking

The screenshot displays a Windows desktop environment. On the left, a browser window is open to 'sorteosrd.com'. Overlaid on the browser is the Windows Task Manager window, which is showing the Performance tab. The Task Manager window displays the following system metrics:

Category	Value
CPU Usage	4%
Physical Memory (MB)	2.06 GB
System	
Total	8191
Cached	1912
Available	6074
Free	4201
Handles	15173
Threads	625
Processes	42
Up Time	0:00:20:08
Commit (GB)	2 / 15
Kernel Memory (MB)	
Paged	178
Nonpaged	40

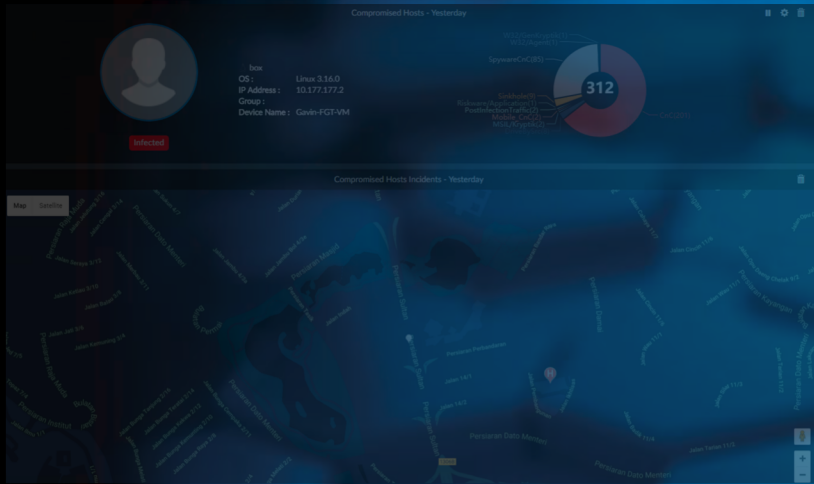
At the bottom of the Task Manager window, it shows: Processes: 42, CPU Usage: 4%, Physical Memory: 25%.

On the right side of the desktop, the Process Explorer window is open, displaying a list of running processes. The processes listed include:

Process	CPU	Private Bytes	Working Set	PID	Description	Company
System Idle Process	86.04	0 K	24 K	0		
System	0.39	264 K	13,192 K	4		
csrss.exe	< 0.01	2,128 K	4,324 K	340		
wininit.exe		1,464 K	4,452 K	376		
csrss.exe	0.80	2,092 K	7,652 K	392		
winlogon.exe		2,732 K	7,072 K	452		
explorer.exe	1.18	22,860 K	46,328 K	2024	Windows Explorer	Microsoft C
procexp64.exe	0.71	12,432 K	23,312 K	536	Sysinternals Process Explorer	Sysinterna
firefox.exe	5.28	109,432 K	151,632 K	1572	Firefox	Mozilla Co
firefox.exe	1.01	75,640 K	104,308 K	1968	Firefox	Mozilla Co
firefox.exe		26,004 K	50,300 K	688	Firefox	Mozilla Co
firefox.exe		22,292 K	38,540 K	2672	Firefox	Mozilla Co
taskmgr.exe	0.85	2,756 K	8,844 K	3384	Windows Task Manager	Microsoft C

The Process Explorer window also shows system performance metrics at the bottom: CPU Usage: 13.96%, Commit Charge: 16.80%, Processes: 42, Physical Usage: 25.84%.

FortiGuard Labs @ fortiguard.com





ZERO-DAY RESEARCH - MORE

Fortinet Discovers Naver Whale Browser UnQuoted Service...

FG-VD-18-027 (Naver) - Jun 28, 2018

Fortinet Discovers Naver Whale Browser DLL Preloading...

FG-VD-17-189 (Naver) - Jun 28, 2018

Fortinet Discovers Tresorit for Windows DLL PreLoading...

FG-VD-18-053 (Tresorit) - Jun 26, 2018

Fortinet Discovers VyprVPN Unquoted Service Path Privilege...

FG-VD-18-049 (Golden Frog) - Jun 22, 2018

Fortinet Discovers Unprotected Wi-Fi Credentials in...

FG-VD-18-074 (Shenzhen Lingun Intelligent Technology) - Jun 22, 2018

Fortinet Discovers Telesquare SDT-CS3B1/SDT-CW3B1 Backdoor...

FG-VD-18-106 (Telesquare) - Jun 20, 2018

Fortinet Discovers Microsoft Windows Webservice Library...

FG-VD-18-003 (Microsoft) - Jun 12, 2018

Fortinet Discovers Microsoft Windows Code Integrity...

FG-VD-18-013 (Microsoft) - Jun 12, 2018

IMPORTANT ADVISORY

Fortinet Discovers Naver Whale Browser UnQuoted Service Path Vulnerability

THREAT BRIEF

FortiGuard Threat Intelligence Brief - June 29, 2018

UPDATES

ANTI-VIRUS 8 hours ago

MOBILE SERVICE 8 hours ago

INTRUSION PROTECTION 4 days ago

APP CONTROL 3 days ago

ANTI-SPAM 7 hours ago

WEB FILTER 7 hours ago

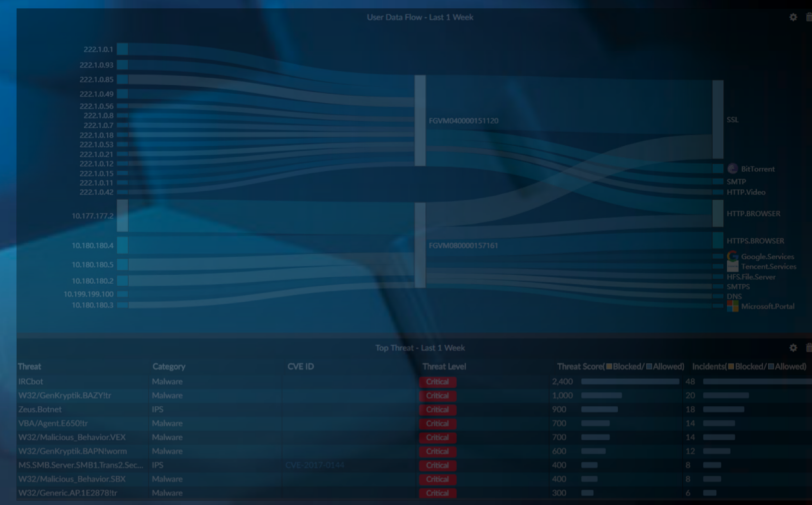
WEB SECURITY 4 days ago

ENDPOINT VULN PROTECTION 19 days ago

INTERNET SERVICES DB 3 days ago

BOTNET IP REPUTATION DB 10 days ago

INDICATORS OF COMPROMISE 1 day ago



THREAT LANDSCAPE REPORT Q2 2018

MINI FOCUS: A GANDER AT GANDCRAB

Many malware incidents under the W32/Gandcrab malware family have been linked to the GandCrab ransomware. Our threat intelligence analysts have identified the operational details to help you understand the threat and its impact on your network. This report is intended for security professionals, researchers, and analysts.

The authors of GandCrab are the first group to reveal their ransomware. It also appears that they use the Agile development methodology to create their malware. This allows them to quickly adapt to changes in the threat landscape. The authors of GandCrab are also known for their ability to create custom malware for specific targets. This allows them to bypass security measures and reach their intended targets.

GandCrab 2.0 variants were first reported during Q2. It is the largest threat in the wild and threat actors expect to see many more. This is because it is easy to use and has a large number of users. It is also easy to use and has a large number of users.



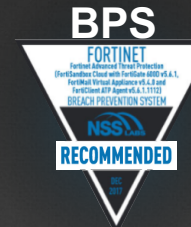
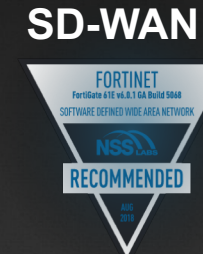
NSS Labs 3rd-Party Testing

Independent Testing



9

Recommendations
out of 9!



A nighttime aerial view of Ulaanbaatar, Mongolia. The city is illuminated with various lights, including streetlights and building lights. A prominent feature is a large, curved, modern building with a blue and white facade, illuminated with blue lights. In the center, a river flows through the city, reflecting the lights. The sky is dark, and the overall atmosphere is vibrant and modern.

баярлалаа