FortiGuard Labs Threat Landscape Highlights

MNSEC 2018

2018 Threat Landscape Predictions

FortiGuard Labs

PREDICTION:

NEXT-GEN MORPHIC MALWARE


CYBER
GRAND CHALLENGE
DARPA
CYBER
DARPA
SCORING
INTEGRITY
MAYHEM
SECURE

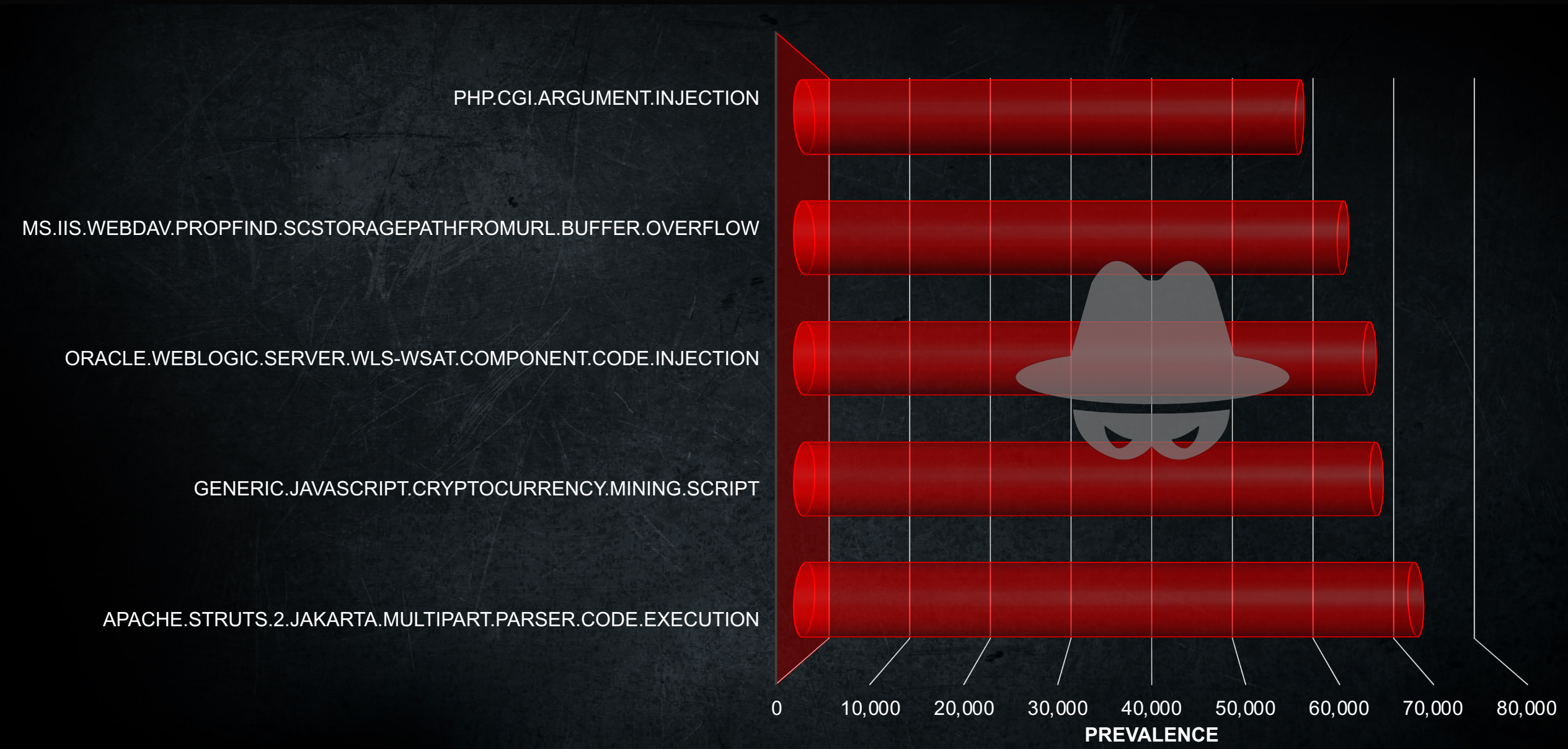

PREDICTION:
CRITICAL INFRASTRUCTURE TO THE FOREFRONT


[HACKING] AMERICA
OFFICIALS: HUNDREDS OF U.S. ELECTRIC PLANTS HACKED
CNBC

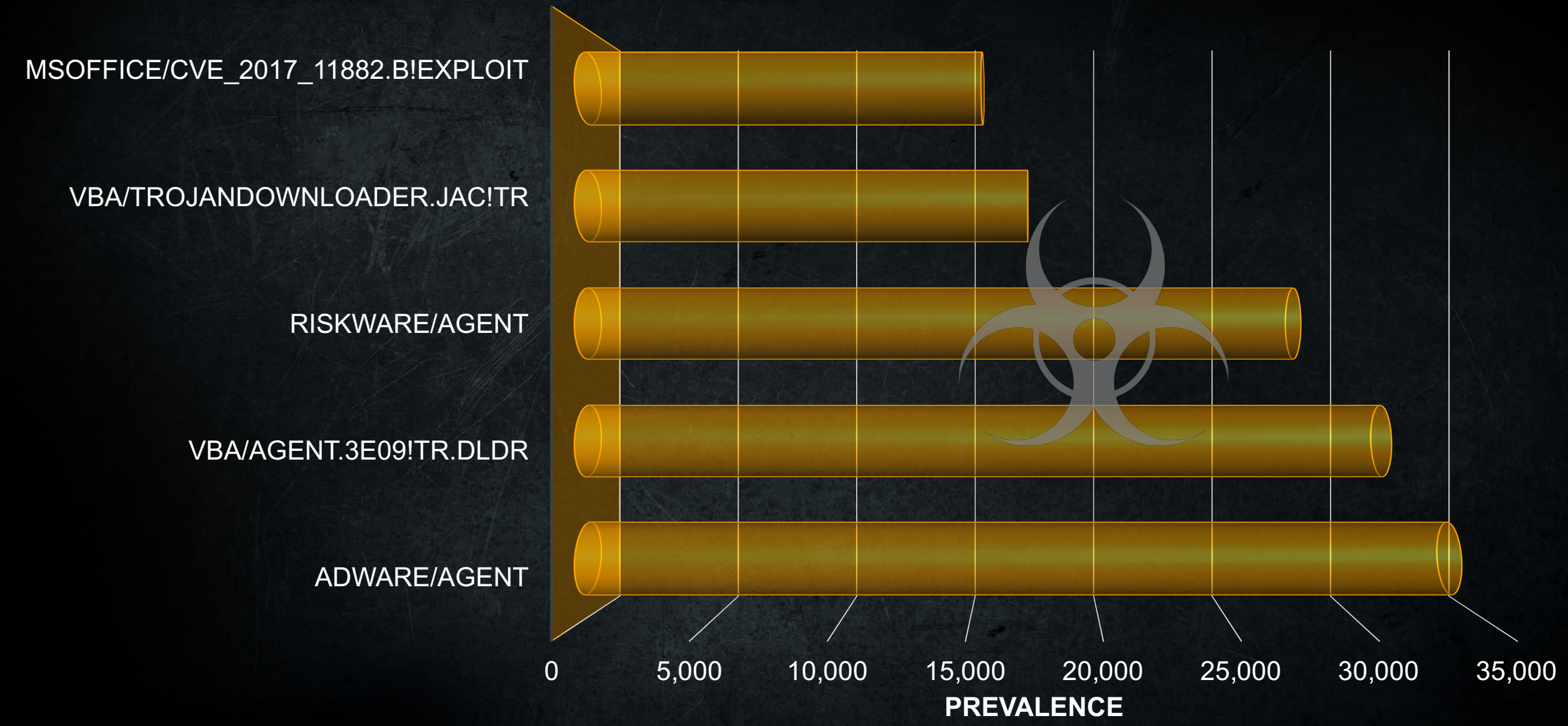
FortiGuard Labs Threat Telemetry

Global and Mongolia – 2018 (Thus Far)

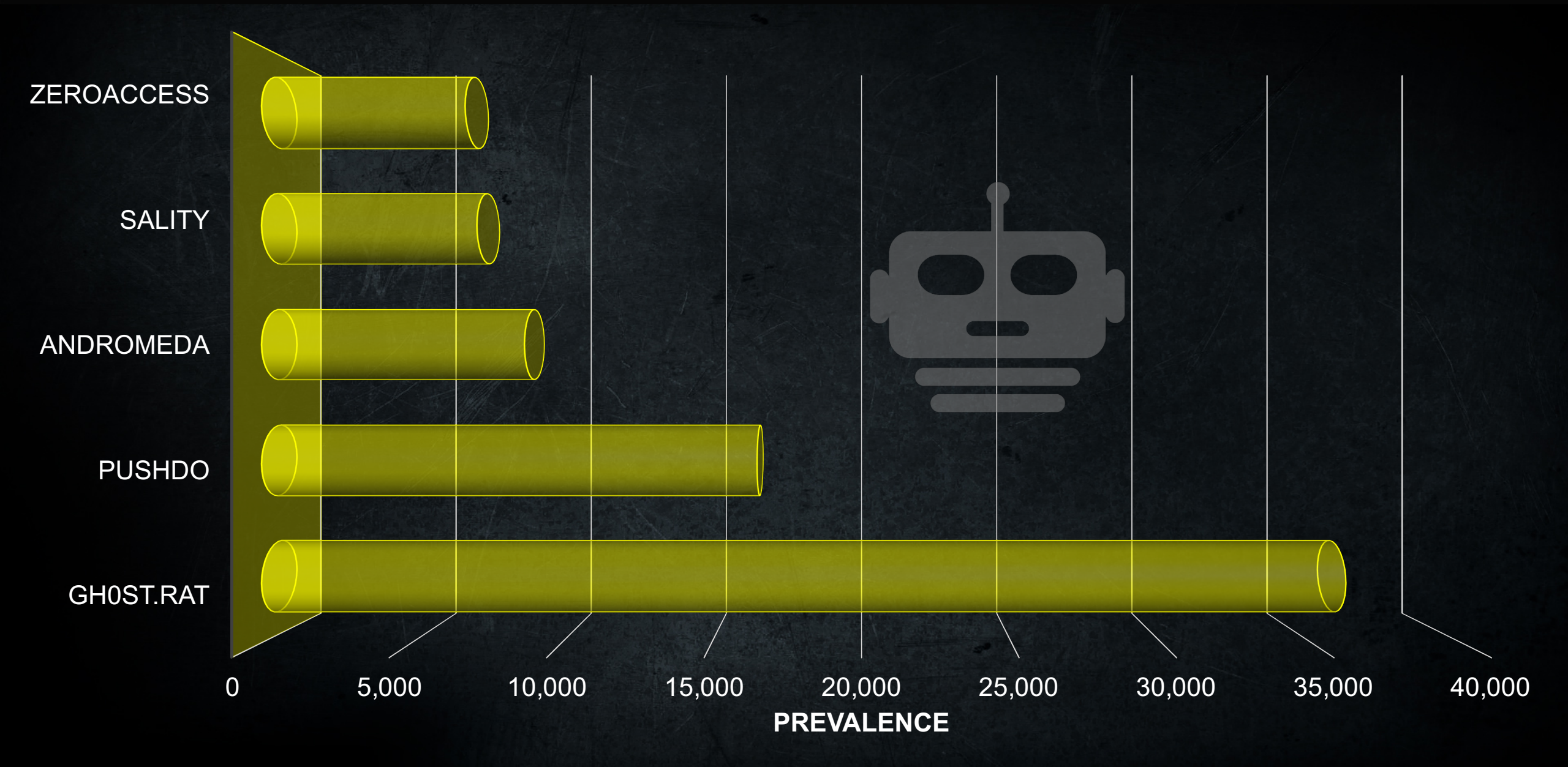
Top 5 Prevalent Attacks – Global



Top 5 Prevalent Malware – Global

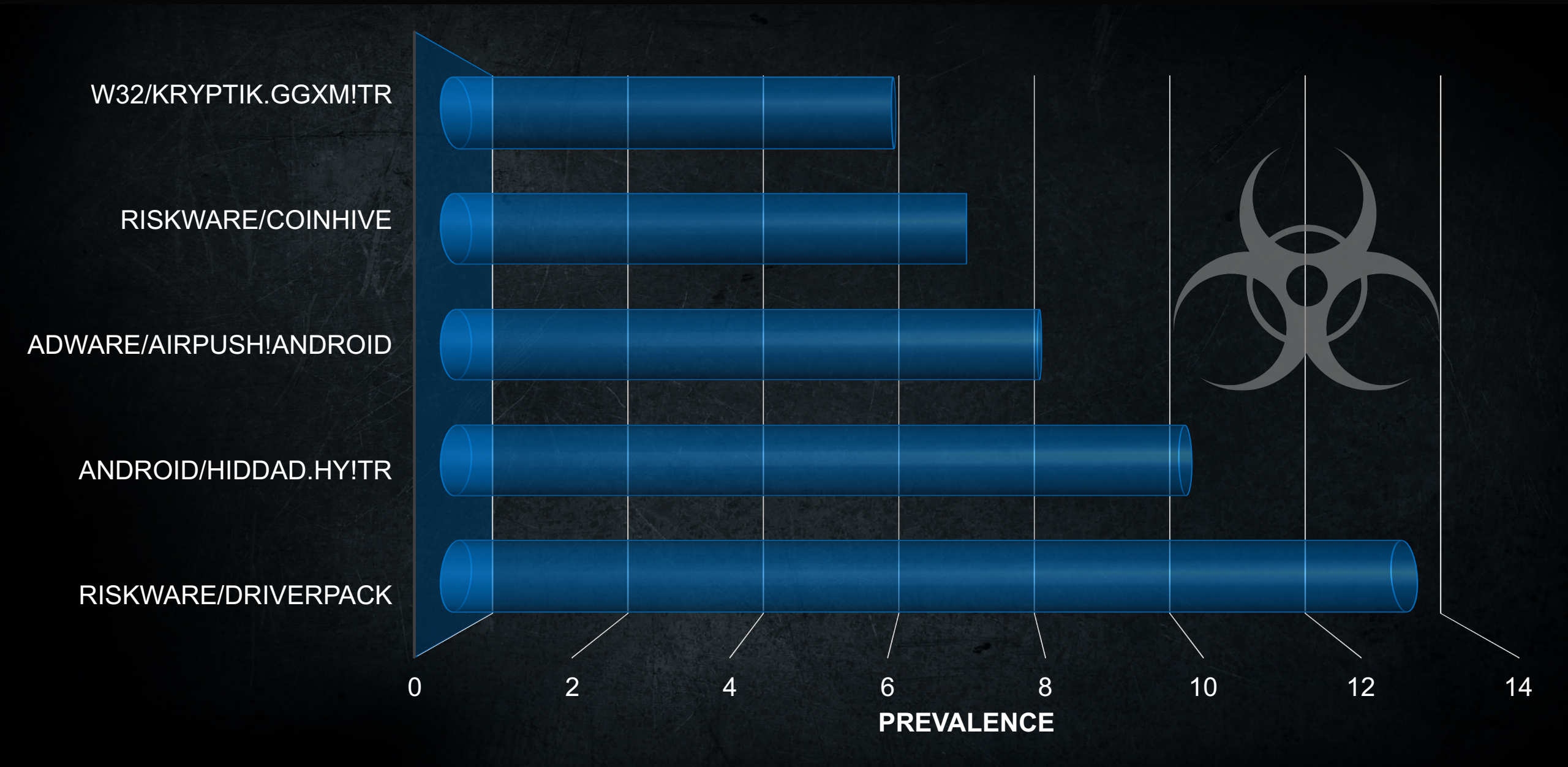


Top 5 Prevalent Botnets – Global

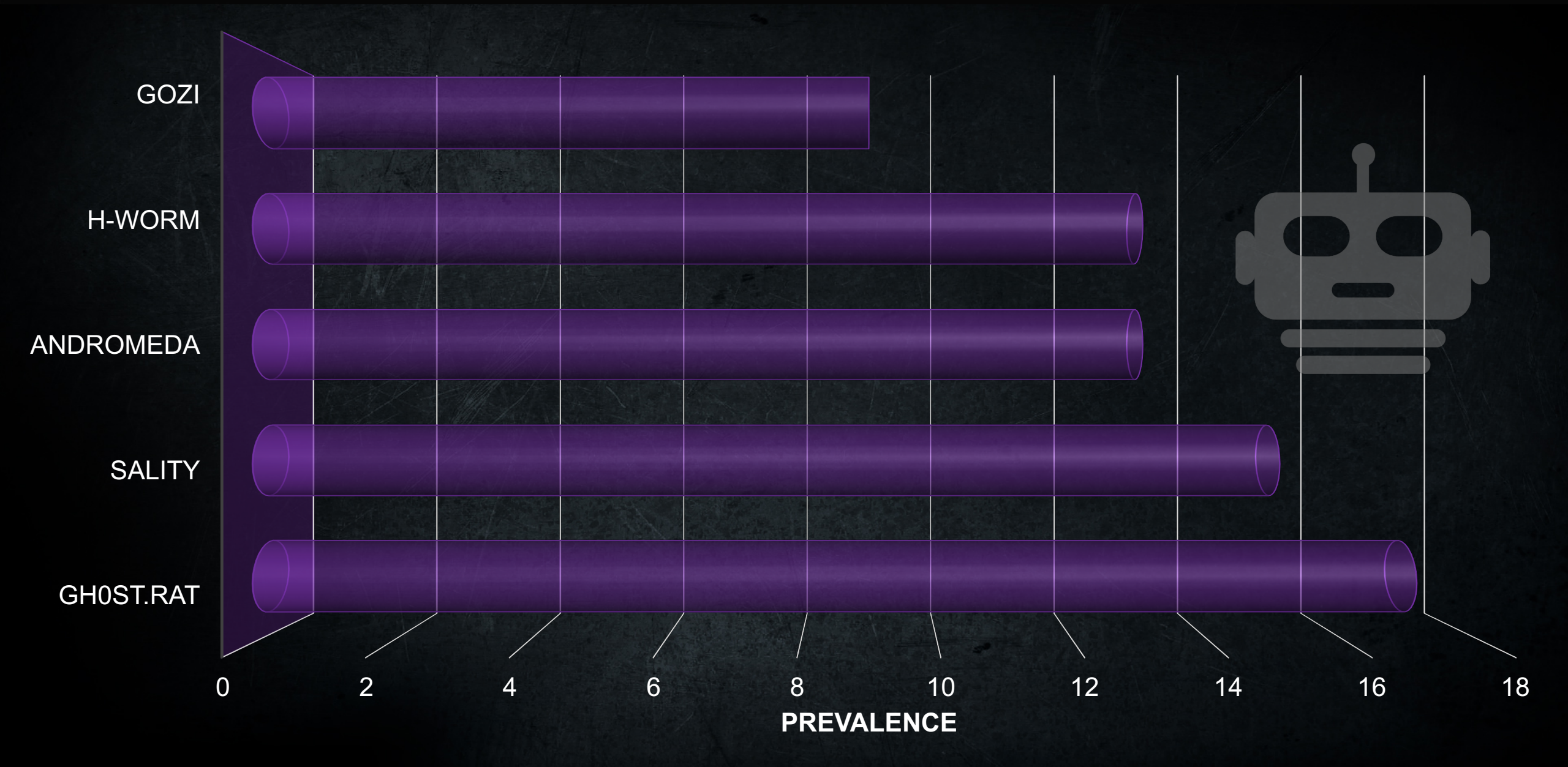


Top 5 Prevalent Attacks – Mongolia

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

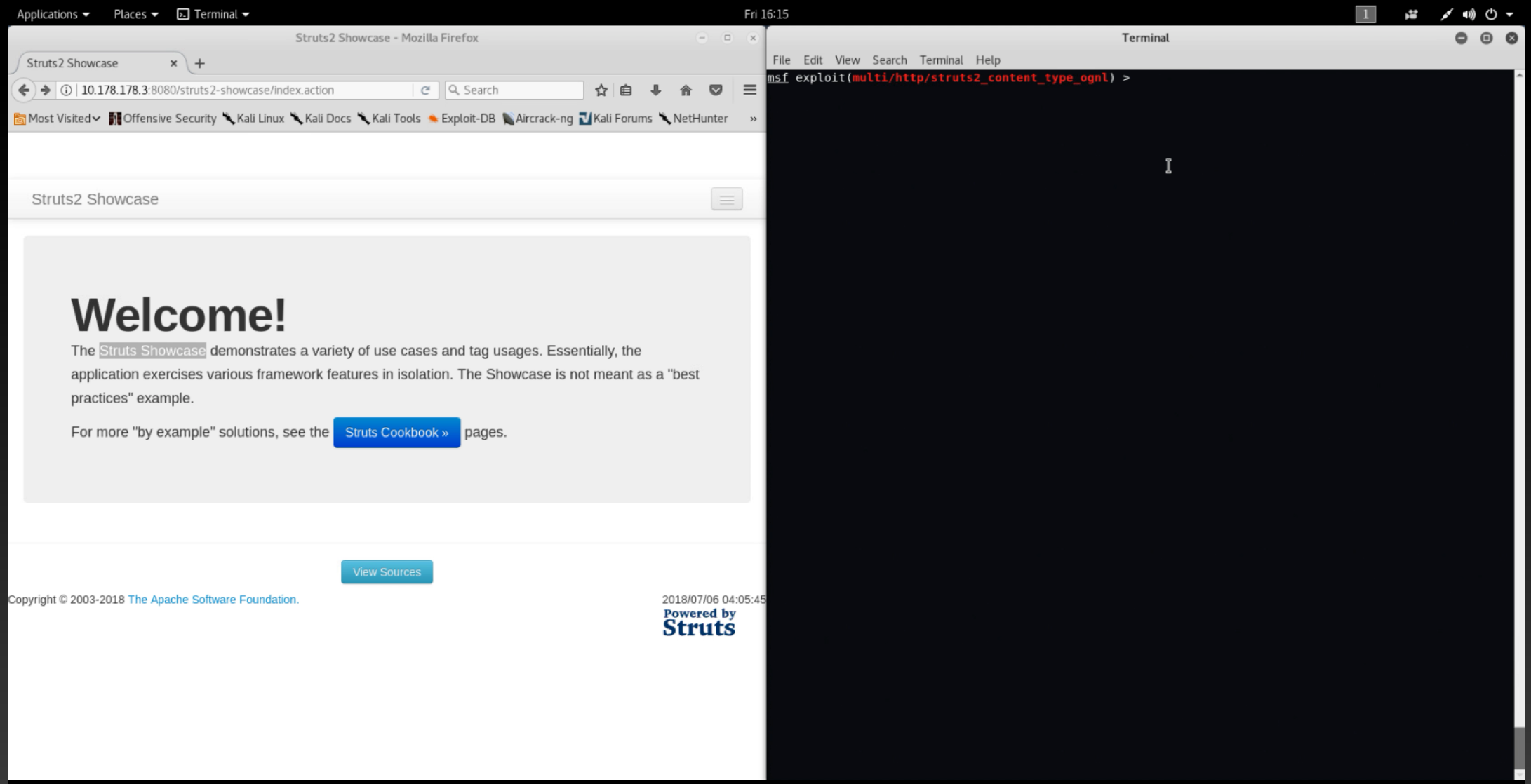
96%

SAW SEVERE EXPLOITS

ONLY **5.7%**

OF KNOWN VULNERABILITIES **WERE TARGETED**

CVE-2017-5638 – Apache Struts 2 RCE



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

THREAT RESEARCH

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 er
This article provides a basic overview of this malicious campaign, and points

Spam Campaign

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

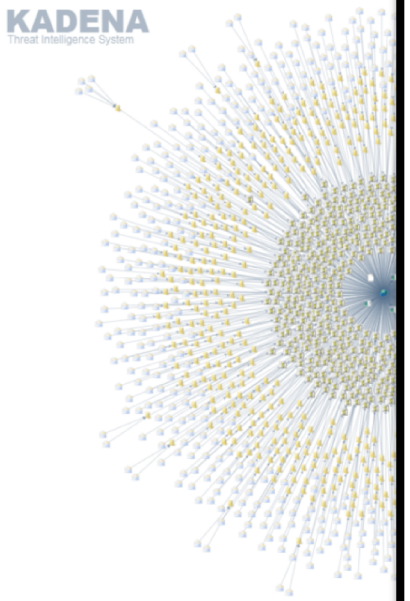


Fig.1 KTIS visualization of the spam

THREAT RESEARCH

GandCrab V3 Accidentall Systems with New 'Ch 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 distribut
previous article. At the end of last month, FortiGuard Labs discovered a new spam wave from the same campa
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.

THREAT RESEARCH

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 us
Malicious pages are currently being injected into legitimate websit

It has been over two months since GandCrab has undergone a major up
structure, its major purposes are practically the same. While some of the
place. Noticeably, the wallpaper change that had been added in the prev
biggest change, however, is the switch from using RSA-2048 to the muc
by the Petya ransomware in the past. Furthermore, it has done away wit
means it is now able to encrypt users that are not connected to the Inter

Note: Thanks to David Maciejak, Director of FortiGuard Research Team,

Note: Read previous research on this topic.

Compromised Websites Serve GandCrab V4.0

The malware was reportedly seen being distributed through compromise
WordPress is a favourite target of exploitation. In fact, for this latest relea
pages (a few of which are shown in the figure below).

THREAT RESEARCH

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**

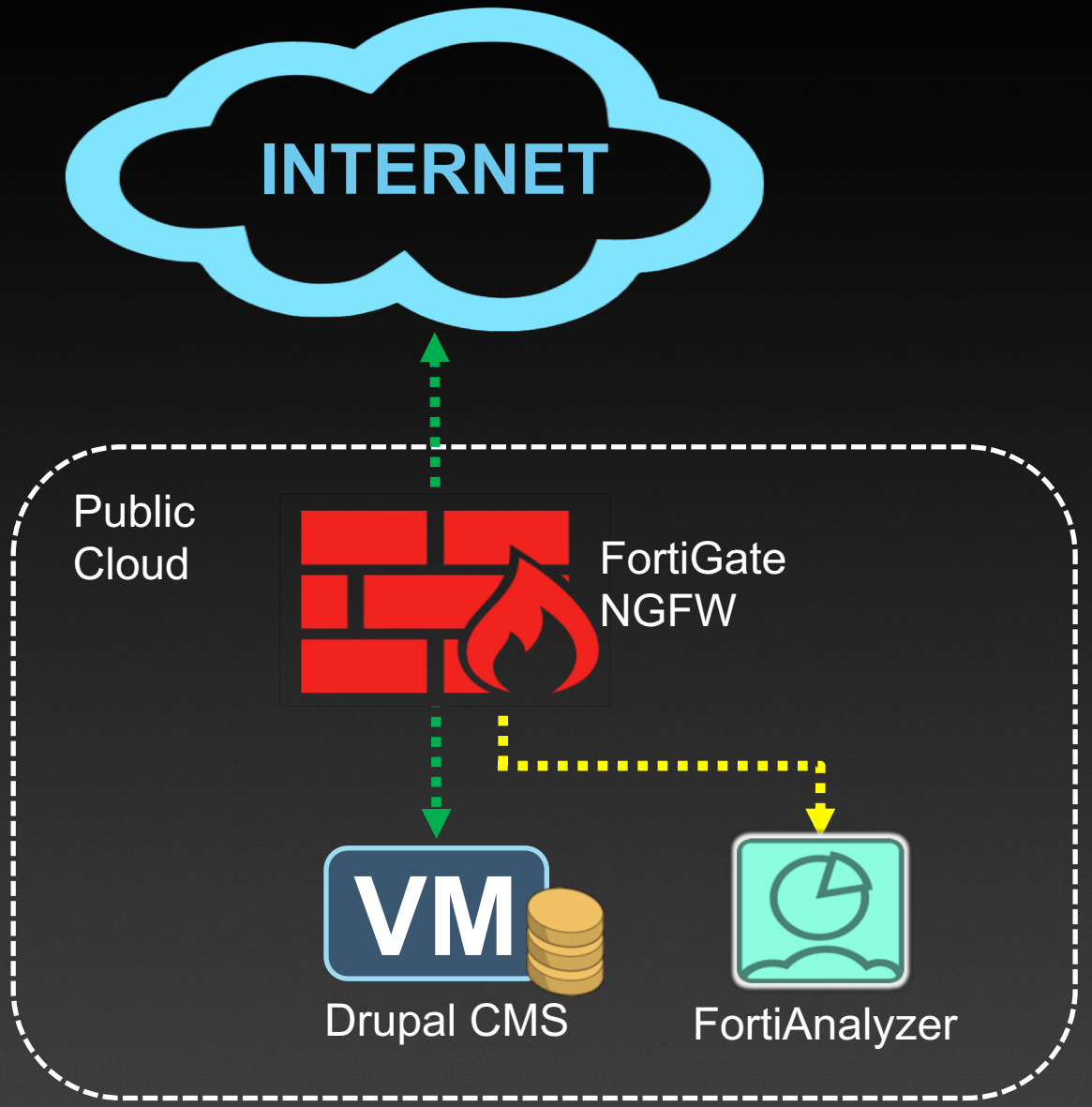
ESPECIALLY POPULAR CRYPTOJACKING TARGETS ARE **MEDIA DEVICES DUE TO POWERFUL GPUS**

Web Honeypot

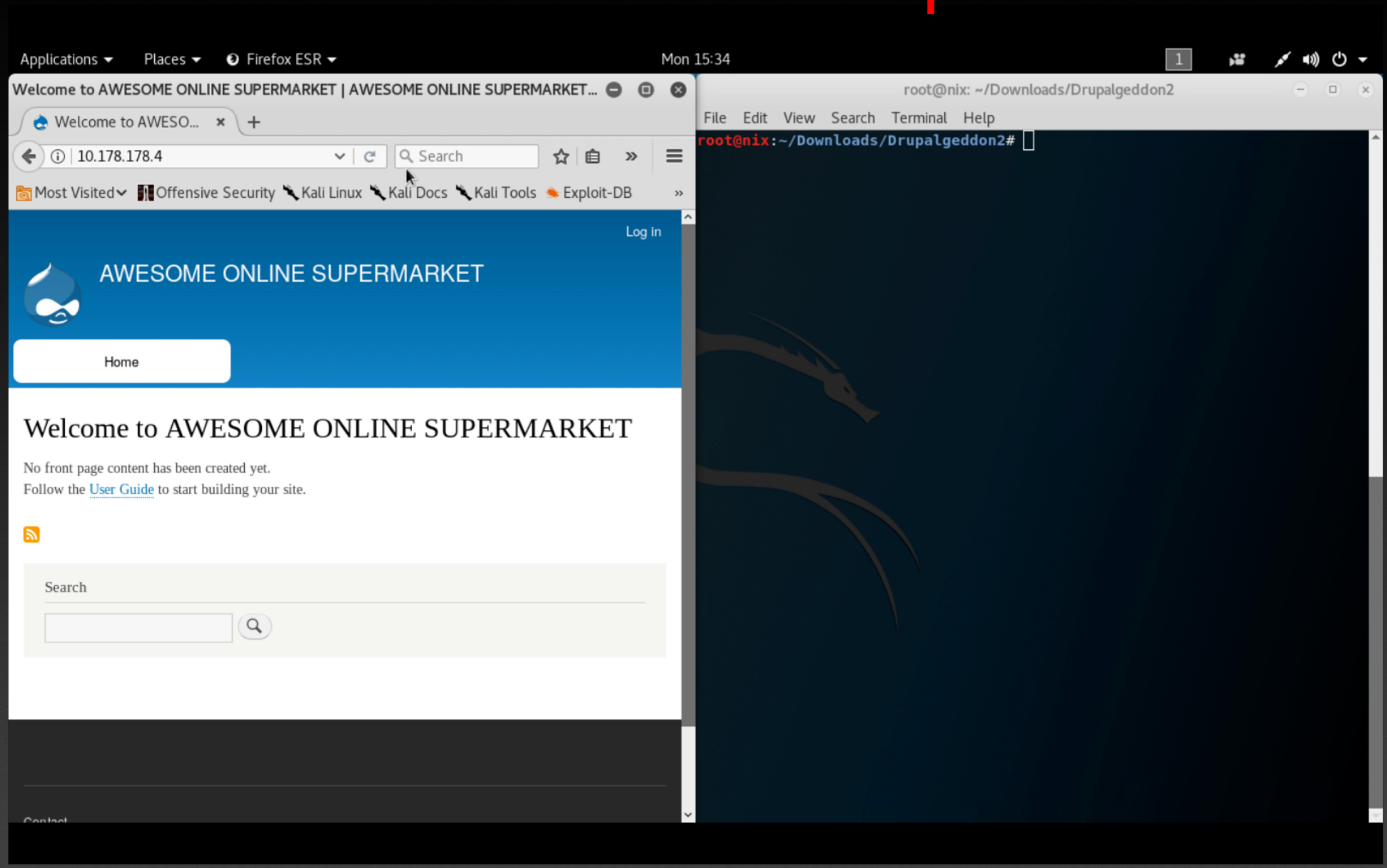
Drupal CMS deployed on a Linux Instance

FortiGate NGFW in **Monitoring Mode**

FortiAnalyzer for Centralized Reporting



CVE-2018-7600 - Drupal RCE

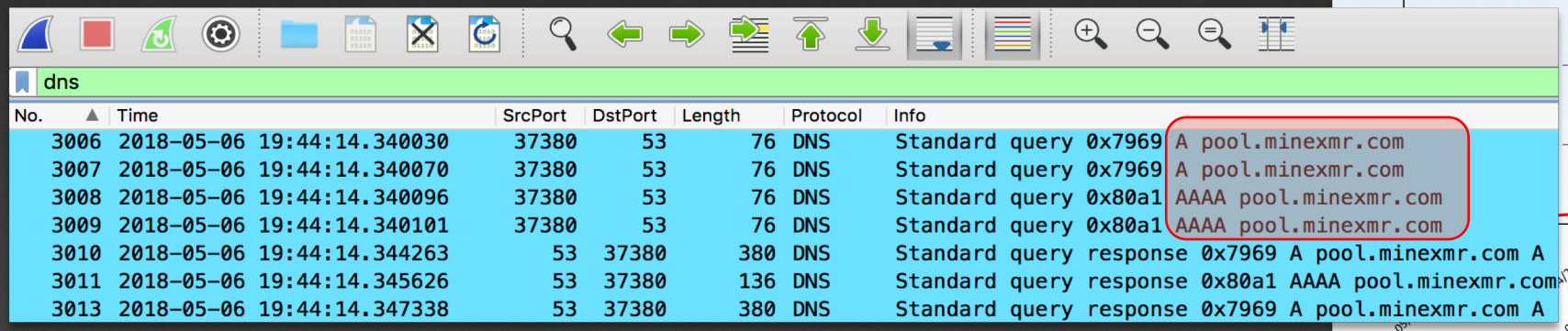


Server Side Cryptojacking

Add Filter | All Devices | Custom... | May 02 To May 07

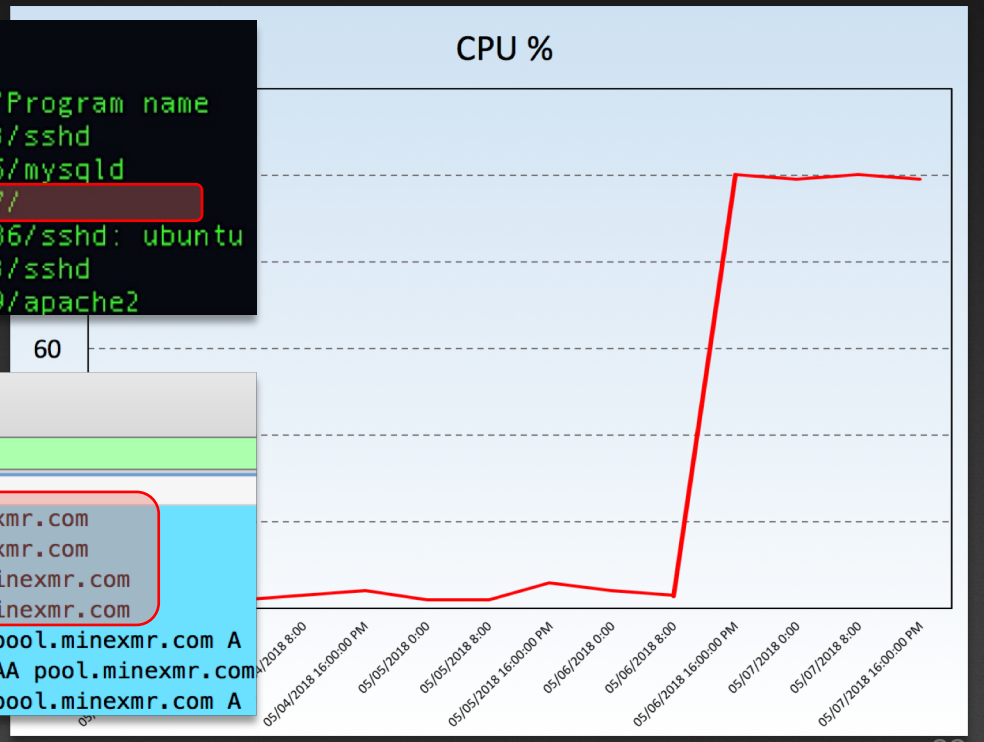
#	Threat	Category	Threat Level
1	Drupal.Core.Form.Rendering.Component.Remote.Code.Execution	IPS	Critical
2	Oracle.WebLogic.Server.wls-wsat.Component.Code.Injection	IPS	Critical
3	MS.IIS.WebDAV.PROPFIND.ScStoragePathFromUrl.Buffer.Overflow	IPS: CVE-2017-7269	Critical
4	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	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                 :5555   ESTABLISHED 9387/
tcp        0    296                :22                    :54787  ESTABLISHED 13686/sshd: ubuntu
tcp6       0      0 :::22                   :::*                    LISTEN      1013/sshd
tcp6       0      0 :::80                   :::*                    LISTEN      8009/apache2
```

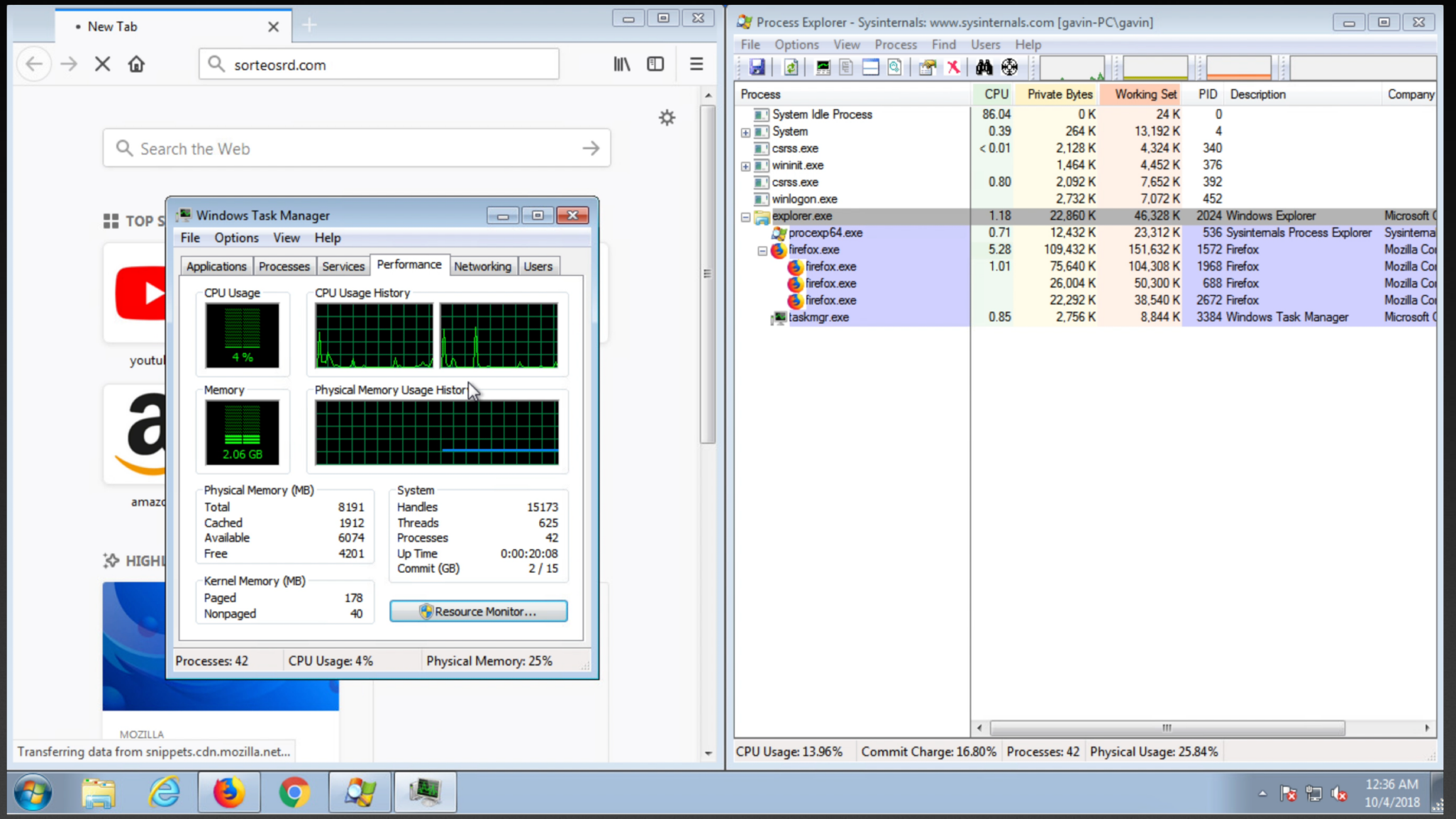


dns

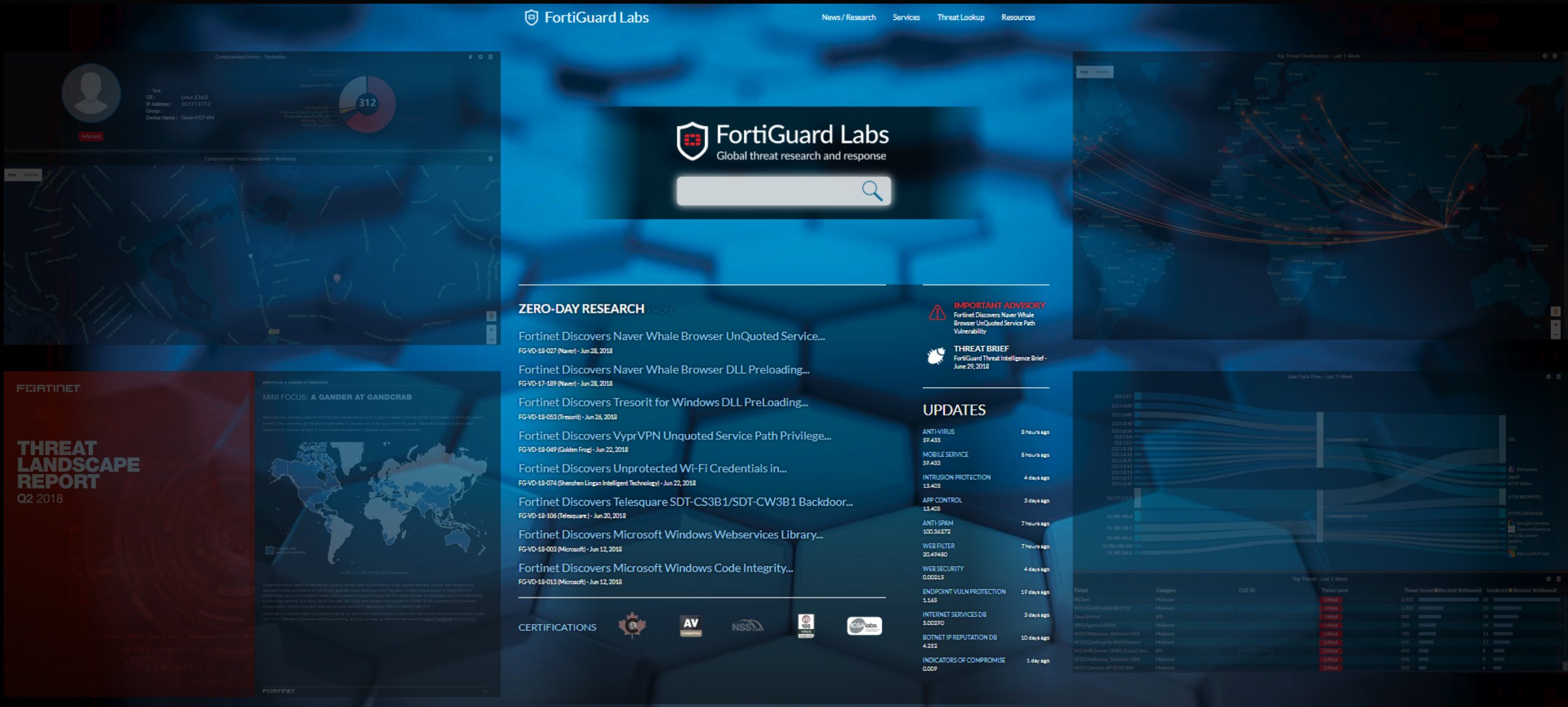
No.	Time	SrcPort	DstPort	Length	Protocol	Info
3006	2018-05-06 19:44:14.340030	37380	53	76	DNS	Standard query 0x7969 A pool.minexmr.com
3007	2018-05-06 19:44:14.340070	37380	53	76	DNS	Standard query 0x7969 A pool.minexmr.com
3008	2018-05-06 19:44:14.340096	37380	53	76	DNS	Standard query 0x80a1 AAAA pool.minexmr.com
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



FortiGuard Labs @ fortiguard.com



NSS Labs 3rd-Party Testing

Independent Testing

9 Recommendations out of 9!

NGFW

NGIPS

DCIPS

DCSG

SD-WAN

BDS

AEP

WAF

BPS