The AlienVault Blogs: Taking On Today's Threats

LATEST
The most recent posts from across the AlienVault blogs.
Subscribe: Via Email | RSS

LABS
Late-breaking discoveries and in-depth analysis.
Subscribe: Via Email | RSS

HOW-TO
Practical, how-to advice, tips and guidance.
Subscribe: Via Email | RSS

Blog Highlights | Labs Research | Security Essentials

Operation BlockBuster unveils the actors behind the Sony attacks

Search AlienVault Blogs

Jaime Blasco
February 24, 2016

SHARE THE LOVE

Today, a coordinated coalition involving AlienVault and several other security companies led by Novetta is announcing Operation BlockBuster. This industry initiative was created to share information and potentially disrupt the infrastructure and tools from an actor named the Lazarus Group. The Lazarus Group has been responsible for several operations since at least 2009, including the attack that affected Sony Pictures Entertainment in 2014.

Part of our research on this actor was presented at the Kaspersky Security Analyst Summit (SAS) in Tenerife, Spain on February 9th, 2016 as a joint talk between AlienVault and Kaspersky's Global Research and Analysis Team.

In the research that AlienVault and Kaspersky collaborated on, we attributed several campaigns to this actor. Armed with some of the indicators that US-CERT made public after the Sony attack, we continued to analyze different campaigns in 2015 that we suspected were being launched by the same actor. Eventually we were also able to attribute previous activity to the same attackers including:

→ Sony Pictures Entertainment - 2014

→ Operation DarkSeoul - 2013

→ Operation Troy - 2013

→ Wild Positron / Duuzer - 2015

Besides several campaigns were the Lazarus group has utilized wipers to perform destructive attacks, they have also been busy using the same tools to perform data theft and cyber espionage operations.

Today, as part of the Operation BlockBuster release, we want to share some of our findings and TTP's from the Lazarus Group that allowed us to link and attribute all the campaigns and tools into the same cluster of activity. We highly recommend that you read the comprehensive report Novetta published today that includes details on the project's scope and the more than 45 malware families identified, and includes signatures and guidance to help organizations detect and stop the group's actions.

FEATURED CONTENT

IDS for Security Analysts: How to Get Actionable Insights from your IDS

Watch Now ▶

Encryption/Shared keys

One of the key findings that gave us the opportunity to link several families to the same actors was finding a dropper that the attackers use. This dropper contains a compressed resource (ZIP) with the name “MYRES” that is protected by a password. The attackers have reused the same password in different occasions and we were able to find droppers containing different families used by the group.

```
21313233 34353637 38393020 64676874 64687472 | !1234567890 dghtdhtr
6867666A 6E756924 255E5E26 66647400 4D005900 | hgfjnui$%^^&fdt M Y
52004500 53000000 6F70656E 00000000 77620000 | R E S   open    wb
6D736474 63767472 652E6261 74000000 3A4C310D | msdtcvtre.bat   :L1
0A64656C 20222573 220D0A69 66206578 69737420 |  del "%s"  if exist
22257322 20676F74 6F204C31 0D0A6465 6C202225 | "%s" goto L1  del "%
73220D0A 00000000 25007300 25007300 00000000 | s"      % s % s
53006300 68006500 64007500 6C006500 68006C00 | S c h e d u l e h l
70000000 53006F00 66007400 77006100 72006500 | p   S o f t w a r e
5C004D00 69006300 72006F00 73006F00 66007400 | \ M i c r o s o f t
5C005700 69006E00 64006F00 77007300 5C004300 | \ W i n d o w s \ C
```

This actor also reuses the code libraries they utilize to perform RSA encryption. We were also able to find the exact same public key in multiple variants.

Batch scripts

This actor often uses BAT files that share the same skeleton in order to delete the initial files after infection.

```
63006500 73000000 6F70656E 00000000 | c e s   open
3A4C310D 0A64656C 202F4620 22257322 | :L1  del /F "%s"
0D0A6966 20657869 73742022 25732220 |  if exist "%s"
676F746F 204C310D 0A64656C 202F4620 | goto L1  del /F
22257322 0D0A0000 77620000 6D736474 | "%s"    wb  msdt
63767472 652E6261 74000000 50006300 | cvtre.bat   P c
```

We have seem them reuse this technique across multiple droppers and payloads.

Obfuscation functions

The Lazarus Group uses a few different methods to obfuscate API functions and dynamically load them. One of them consist on using a simple XOR schema.

You can find other examples of API function obfuscation in the Novetta report.

Network communications

This actor has different malware families in their toolset that implement a similar C&C protocol. The protocol looks like TLS but it is in fact a “fake” TLS protocol that mimics it.

One of the characteristics we have identified is how they choose the values for certain fields when generating “TLS” packets, especially the ClientHello packet.

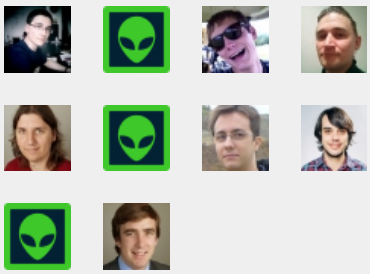
Beginner’s Guide to Open Source Intrusion Detection Tools

Read Now ▶

Six Steps to SIEM Success

Watch Now ▶

OUR AUTHORS:

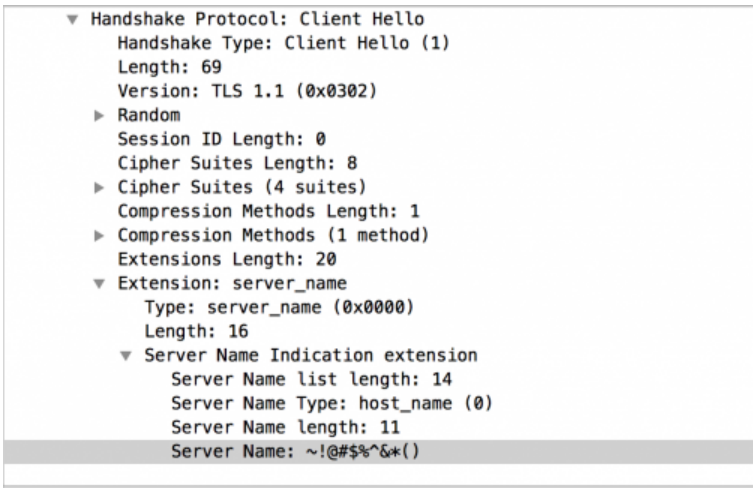


TAGS:

0day alienvault android apt attacks botnet c&c china compliance correlation credit cards cve-2012-0158 directives directory objects exploit ids installer internet explorer kernel objects macosx malware nessus office ossec ossim otx pci phishing plugins plugx pos ransomware rat reverse engineering sandbox scada siem snort ssl sykipot targeted attacks threat data threat intelligence trojan tutorial vulnerabilities vulnerability windows yara zeroday

We have identified different families exhibiting slightly different behaviors:

→ Using a static “Server Name” extension in the client_hello packet: “^~!@#$%^&*()”



→ Choosing between “www.amazon.com” and “www.google.com” for the “Server Name” value.

→ Randomly choosing one of the following items for the “Server Name” value (this list can vary across different samples):

wwwimages2.adobe.com

www.paypalobjects.com

www.paypal.com

www.linkedin.com

www.apple.com

www.amazon.com

www.adobetag.com

windowslive.tt.omtrdc.net

verify.adobe.com

us.bc.yahoo.com

urs.microsoft.com

supportprofile.apple.com

support.oracle.com

support.msn.com

startpage.com

sstats.adobe.com

ssl.gstatic.com

ssl.google-analytics.com

srv.main.ebayrtm.com

skydrive.live.com

signin.ebay.com

securemetrics.apple.com

secureir.ebaystatic.com

secure.skypeassets.com

secure.skype.com

secure.shared.live.com

secure.logmein.com

sc.imp.live.com

sb.scorecardresearch.com

s1-s.licdn.com

s.imp.microsoft.com

pixel.quantserve.com

p.sfx.ms

mpsnare.iesnare.com

login.yahoo.com

login.skype.com

login.postini.com

login.live.com

l.betrad.com

images-na.ssl-images-amazon.com

fls-na.amazon.com

extended-validation-ssl.verisign.com

daw.apple.com

csc.beap.bc.yahoo.com

by.essl.optimost.com

b.stats.ebay.com

apps.skypeassets.com

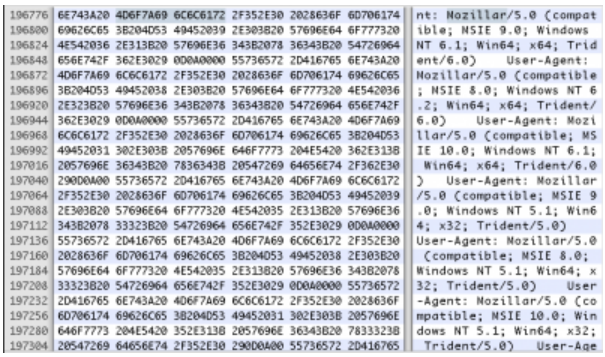
api.demandbase.com

ad.naver.com

accounts.google.com

On the other hand, most of the samples we have analyzed communicate with IP addresses that are part of compromised infrastructure. Since the attackers don't leverage domain names for C2 it makes it hard to pivot using whois data, and passive DNS. In addition, there is no way to sinkhole since there is no domain infrastructure.

Another example is the use of user-agent values that contain the misspelled "Mozillar" string.



Hangul HWP Document Exploits

Hangul is an office suite and word processing application mainly used in South Korea, especially in the government.

We have observed this actor launching spearphishing campaigns with malicious HWP documents as attachments.

An example is a campaign that was launched on September 2015 that used a zeroday vulnerability (CVE-2015-6585) in the Hangul Word processor which was reported by FireEye.

Based on obtained samples and decoy documents we observed that they were likely targeting a wide range of victims including government, industrial and political entities.

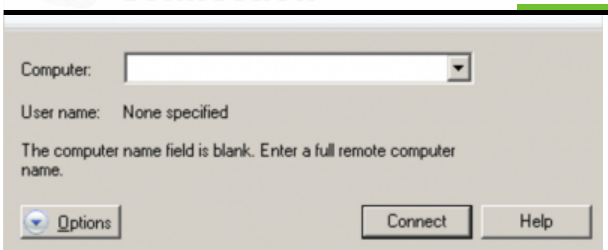
Who We Are
Meet AlienVault
AlienVault Labs
Management Team, Board & Advisors
Customers
Careers

Newsroom
Newsroom Central
Press Coverage
Press Releases
Awards
Events
Blogs

Support & Training
Support Overview
Customer Portal
Health Check Services
Documentation Center
Product Forums
Training
Certification

Partners
Partner Program Overview
Partner Portal
Resellers
MSSPs/MSPs
Implementation Partners
Technology Partners

LOGIN | CONTACT | SUPPORT | MORE
PRODUCTS SOLUTIONS OPEN THREAT EXCHANGE RESOURCES
FREE TRIAL



GET OUR BLOGS DELIVERED TO YOUR INBOX!
GET EMAIL UPDATES
Labs Research
Security Essentials
All Blogs
RSS

Indicators of Compromise

As part of Operation BlockBuster, Novetta is sharing Yara rules and IOC's that you can find at the following website:

Operation BlockBuster

In addition to that we are making the indicators of compromise available in our Open Threat Exchange:

https://otx.alienvault.com/pulse/56cdb68f4637f27567167dce/

CHAT NOW

WEBCAST:
Detect Ransomware Before It's Too Late with AlienVault USM

By now you've probably heard about new ransomware threats like CryptoWall, which encrypts your data and demands payment to unlock it. These threats are delivered via malicious email attachments or websites, and once they execute and connect to an external

command and control server, they start to encrypt files throughout your network. Therefore, spotting infections quickly can limit the damage.

WATCH THE WEBCAST NOW

LEARN MORE:

- 2015 Gartner Magic Quadrant for SIEM: Visionary Aliens
- Intrusion Detection Techniques: Methods & Best Practices
- Botnet Detection and Removal: Methods & Best Practices
- Command and Control Server Detection: Methods & Best Practices
- Distributed Denial of Service Attacks: Protection Methods and Best Practices

Tags:

Blog Home Previous

From the Blog

Jaime Blasco
Feb 24, 2016

Operation BlockBuster unveils the actors behind the Sony attacks

Explore All Blog Posts >

© Copyright 2016 AlienVault, Inc. | Legal | EULA | Privacy Policy