RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: TV-W04

THE RISE OF SUPPLY CHAIN ATTACKS

Craig Williams

Director Outreach
Cisco Talos
@security_craig

RSAConference2018

NOW MATTERS

#RSAC

It started with a phone call…

Nyetya Impact

More than half of major malware attack's victims are industrial targets

Posted Jun 29, 2017 by Taylor Hatmaker (@tayhatmaker)

Ransomware 'Nyetya' behind new global cyber attack: Cisco

BY IANS | **UPDATED:** JUN 28, 2017, 12.00 PM IST

Post a Comment

Lasting Damage and a Search for Clues in Cyberatta

By NICOLE PERLROTH JULY 6, 2017

Key researchers reclassify N suspect destruction was tru

The Detonation

#RSAC

JUNE 27TH, 2017

APRIL 14, 2017
01.175-10.01.176 version of MeDoc is released with a backdoor.

MAY 15, 2017
01.180-10.01.181 version of MeDoc is released with a backdoor.

JUNE 22, 2017
01.188-10.01.189 version of MeDoc is released with a backdoor

8:59:14 UTC
Malicious actor used stolen credentials and "su" to obtain root privileges on the update server.

BETWEEN 9:11:59 UTC AND 9:14:58 UTC
The actor modifies the web server configuration to proxy to an OVH server.

9:14:58 UTC
Logs confirm proxied traffic to OVH.

12:31:12 UTC
The last confirmed proxy connection to OVH is observed. This marks the end of the active infection period.

12:33:00 UTC
The original server configuration is restored.

14:11:07 UTC
Received SSH disconnect from Latvian IP 159.148.186.214

19:46:26 UTC
The OVH server, 176.31.182.167, is wiped using "dd if=/dev/zero", filling the hard drive with 0x00.

The Backdoor

Contacts upd.me-doc.com.ua every 2 mins

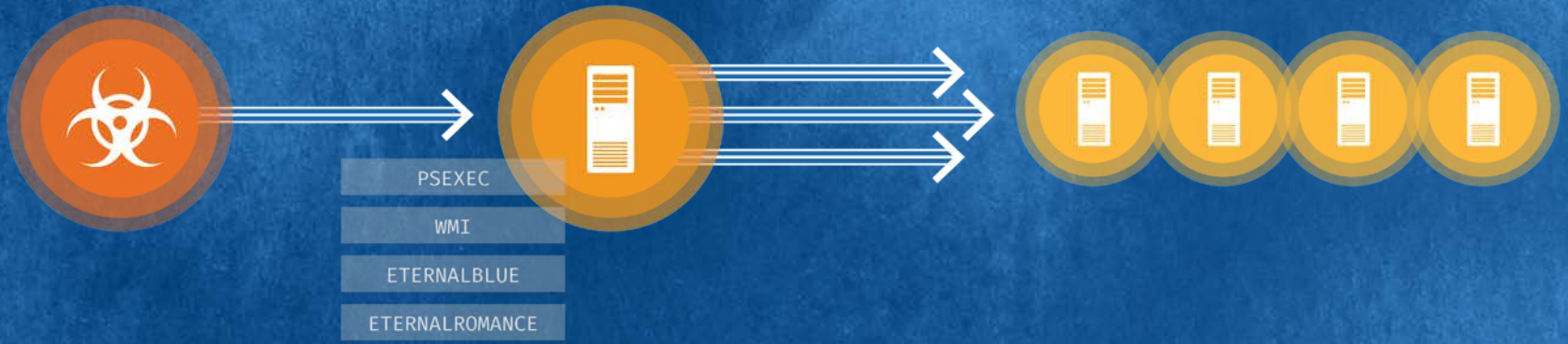
If finds a proxy:

- Retrieve email data from local me-doc
- Wait for & execute commands

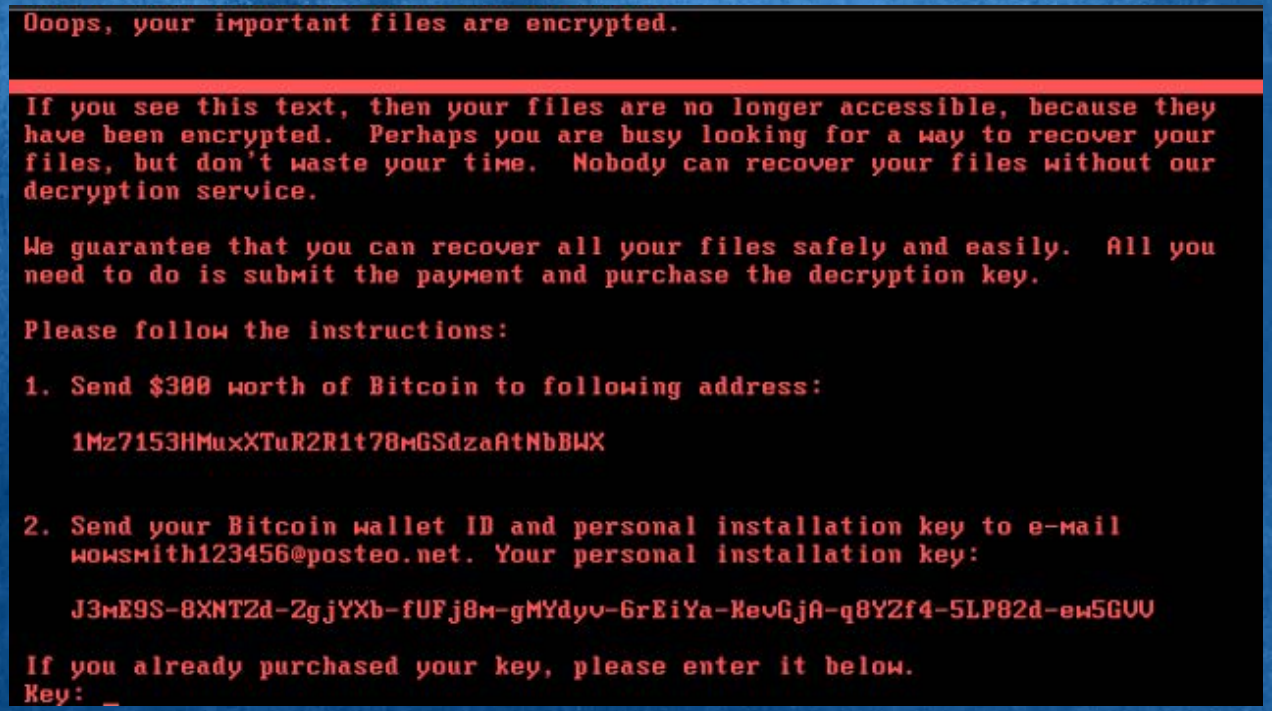
These commands almost certainly used to distribute Nyetya.

Propagation

Scans IP subnet



Payload


Ooops, your important files are encrypted.
If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.
We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1. Send $300 worth of Bitcoin to following address:
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:
J3mE9S-8XNTZd-2gjYXb-fUFj8m-gMYdyv-6rEiYa-KevGjA-q8YZf4-5LP82d-ew5GUV
If you already purchased your key, please enter it below.
Key: _

Genuine Ransomware?

- Single bitcoin wallet means difficult to follow who has paid.
- Single contact email address, now blocked
  - you can’t contact the criminals even if you want to.

- If admin, MBR is overwritten.
- If not admin, wipes first 10 disk sectors.
- If have software “avp.exe” running, wipes first 10 disk sectors.

RSAConference2018

#RSAC

CCleaner Command and Control Causes Concern

Supply Chain Attacks

NEWS

New Havex malware variants target industrial control system and SCADA users

By Lucian Constantin

BRIEF

Maersk says Nyetya cyberattack cost it $300M in revenue loss

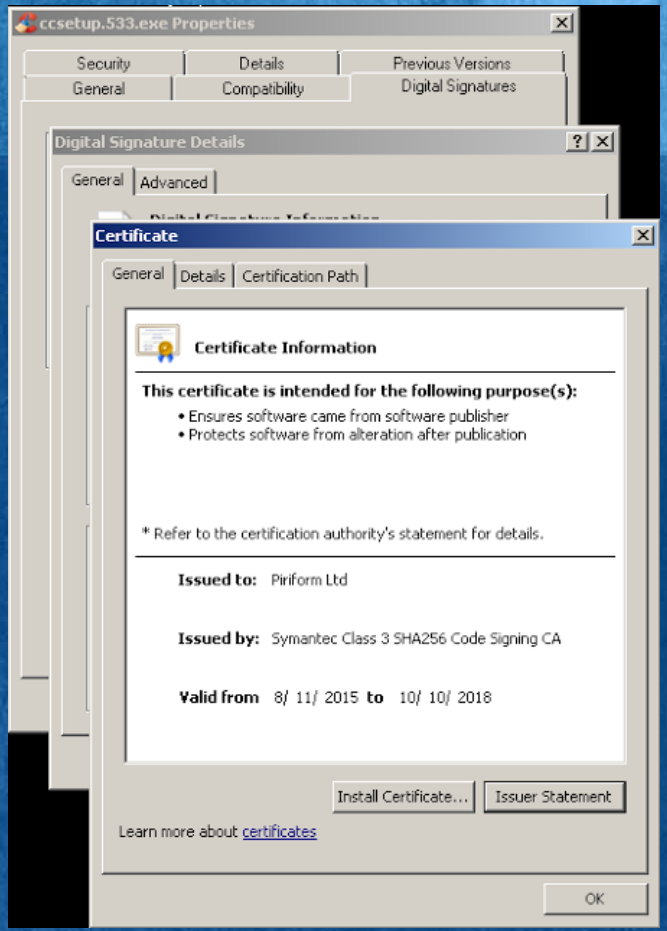
ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS

UPDATE WITH THE DEVIL —

Avast! There's malware in that CCleaner software update

Avast's recent acquisition spreads a backdoor signed with its own certificate.

SEAN GALLAGHER - 9/18/2017, 10:08 AM



Digital Signature of CCleaner 5.33

- presence of a valid digital may be indicative of a larger issue that resulted in portions of the development or signing process being compromised
- this certificate should be revoked and untrusted moving forward

Compilation Artifact

- likely an attacker compromised a portion of development or build environment
- Leveraged access to insert malware into the CCleaner build that was released and hosted by the organization

S:\workspace\ccleaner\branches\v5.33\bin\CCleaner\Release\CCleaner.pdb

Data Collected on Infected Systems

Installed Programs

Adobe Flash Player 23 ActiveX
Adobe Flash Player 26 NPAPI
Adobe Shockwave Player 12.1
CCleaner
CubePDF Utility 0.3.3兌 (x86)
Windows 僪儔僀僶 僷僢働乕僕 - OLYMPUS IMAGING CORP.
Camera Communication Driver Package (09/09/2009 1.0.0.0)
Google Chrome
晉嶺抜姃捁婇攖僜乕僗傷僐僗傷
LanScope Cat MR
Mozilla Firefox 55.0.3 (x86 ja)
Mozilla Maintenance Service
僼僀儖僒僀僘傿乕 Corp.儈僯僠傾僯僢
攄岅岺娄尋媠強丂PDFinder 4.6
Picasa 3
TeamViewer 9
Roxio Central Data
Google Toolbar for Internet Explorer
埆嶌壎zip嵐愙帺梲
Roxio Central Tools
Google Toolbar for Internet Explorer
Java 8 Update 141
UpdateAdvisor(柿懴慉抲) V3.60 L20
eReg
Java Auto Updater
PA-ZS600T
Google Earth Plug-in
Google Update Helper
swMSM
Intel(R) Management Engine Components
堦檻柛價傑乕傾2014
Windows Media Player Firefox Plugin
CubePDF 1.0.0RC7
Fuji Xerox DocuWorks Viewer Light 8
Google 擔柿岅擖椡
iCloud
Security Update for Microsoft Excel 2010 (KB3191907) 32-Bit Edition
Security Update for Microsoft Office 2010 (KB2956063) 32-Bit Edition
Update for Microsoft Office 2010 (KB2589318) 32-Bit Edition

Process List

System
C:\Windows\System32\smss.exe
C:\Windows\System32\csrss.exe
C:\Windows\System32\wininit.exe
C:\Windows\System32\csrss.exe
C:\Windows\System32\services.exe
C:\Windows\System32\lsass.exe
C:\Windows\System32\lsm.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\nvvsvc.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\audiodg.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\SLsvc.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\winlogon.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\nvvsvc.exe
C:\Windows\System32\spoolsv.exe
C:\Windows\System32\svchost.exe
C:\Program Files\Common Files\Adobe\ARM\1.0\armsvc.exe
C:\Program Files\Agilent\IO Libraries Suite\AgilentIOLibrariesService.exe
C:\Program Files\Agilent\IO Libraries Suite\LxiMdnsResponder.exe
C:\Program Files\ESET\ESET Endpoint Antivirus\ekrn.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\svchost.exe

Targeted to Tech Companies

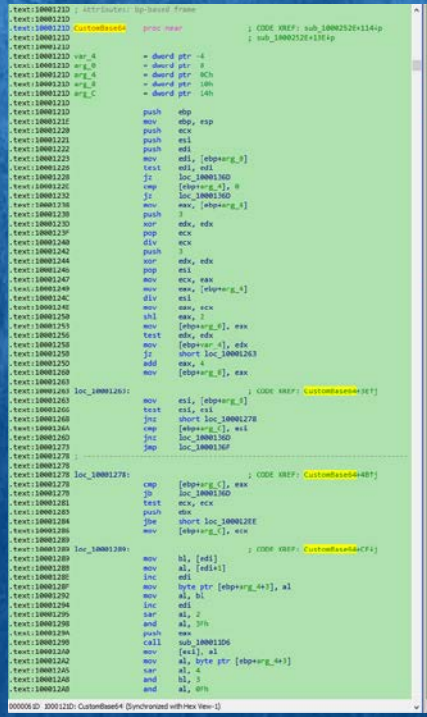

```
$DomainList = array(
"singtel.corp.root",
"htcgroup.corp",
"samsung-breda",
"Samsung",
"SAMSUNG.SEPM",
"samsung.sk",
"jp.sony.com",
"am.sony.com",
"gg.gauselmann.com",
"vmware.com",
"ger.corp.intel.com",
"amr.corp.intel.com",
"ntdev.corp.microsoft.com",
"cisco.com",

"uk.pri.o2.com",
"vf-es.internal.vodafone.com",

"linksys",
"apo.epson.net",
"msi.com.tw",
"infoview2u.dvrdns.org",
"dfw01.corp.akamai.com",
"hq.gmail.com",
"dlink.com",

"test.com");
```

2nd Stage only delivered to 23 specific domains

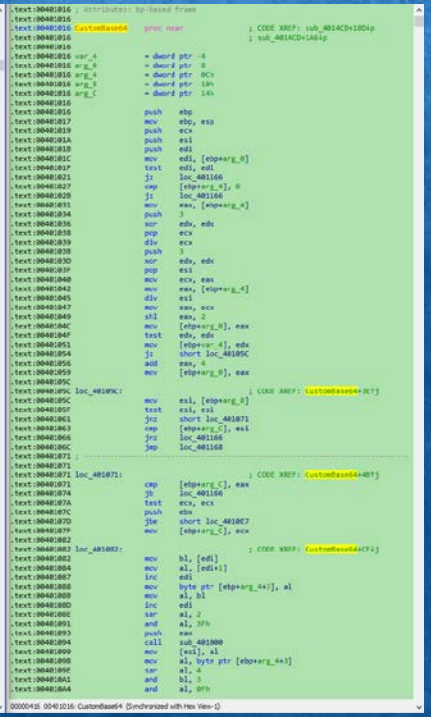
- Database Tracked 2nd Stage Delivery
- No Cisco Devices Delivered 2nd Stage

Code Reuse with Group 72

CCleaner Malware



Group 72 Malware



Who is Group 72

#RSAC

CENTRAL ASIA | EAST ASIA | OCEANIA | SOUTH ASIA | SOUTHEAST ASIA | ECONOMY | DIPLOMACY | ENVIRON

BLOGS | INTERVIEWS | PHOTO ESSAYS | VIDEOS | PODCASTS | MAGAZINE | SUBSCRIBE

CHINA POWER

Report: 'Highly Sophisticated Cyber Espionage' Group Linked to Chinese Intelligence

A new report claims to have uncovered a Chinese hacking group more sophisticated than Unit 61398.

By Shannon Tiezzi
October 29, 2014

Image Credit: Image via Sl

A report issued by private cyber-security firms claims to have unveiled a sophisticated hacking outfit sponsored by the Chinese governme "Axiom" in the report, is said to have targeted everything from government offices in a global campaign over the past six years. A PDF of the full report, titled ""Opera Actor Group Report" can be accessed here.

October 15, 2014

Global security firms cooperate against Chinese hackers

Ten cyber-security companies have cooperated to pool intelligence and combat Chinese APT actors.

For the first time, a group of 10 leading cyber-security companies have joined forces to hit back against an advanced persistent threat (APT) hacker

Global security firms cooperate against Chinese hackers

ninals, but the security
ymantec and FireEye – have
ers and the malware tools

fensive are detailed in a
rm Novetta, which led the group.

New Chinese Intelligence Unit Linked to Massive Cyber Spying Program

Axiom likely a Ministry of State Security spy unit

SHARE TWEET EMAIL

BY: Bill Gertz Follow @BillGertz
October 31, 2014 5:00 am

Google China building in Beijing / AP

A Chinese intelligence unit carried out a massive cyber espionage program that stole vast quantities of data from governments, businesses and other organizations, security analysts who uncovered the operation said Thursday.

The activities of the Chinese unit called the Axiom group began at least six years ago and were uncovered by a coalition of security firms this month.

TALOS

https://blogs.cisco.com/security/talos/threat-spotlight-group-72

RSAConference2018