

The Shadow Brokers

Cyber Fear Game-Changers

PUBLISHED JULY 2017



comae
technologies

Contents

Abstract.....4

Executive Summary 5

Details..... 5

 What is the reason for TheShadowBrokers..... 5

 Finite Data Means Finite Capacity..... 6

 Timeline 8

 Wine of the Month Club Timeline 9

 Timeline Details..... 10

Conclusion..... 18

Abstract

Who are The Shadow Brokers? We have no clue and nobody really does. The Shadow Brokers are one of most controversial groups of this Cyber-Era. The mysterious group emerged mid-summer 2016 when they started to publicly drop tools and operational notes anonymously, that allegedly belonged to the NSA Tailored Access Operations unit. This group referred to itself as The Shadow Brokers and quickly became the NSA's worst nightmare since Edward Snowden.

Previous whistle blowers released documents redacted of sensitive nature, such as authors. But with The Shadow Brokers, what emerged was a different level of dangerous and more aggressive leaks. Which didn't only release highly sensitive tools, but also revealed a wide range of modus operandi that included agents' names and the full disclosure of the NSA's complex (and many argue irresponsible) attack against the backbone of the Middle East's financial institutions. For now, The Shadow Brokers are happy to have the general public guessing their identity and true origins. Is it an intelligence organization running a highly complex set of misdirection and penetration? Is it a second Snowden with access to the NSA's most sensitive cyber weapons? We may never know. What is certain, is that the emergence of The Shadow Brokers is a game-changer and presents a massively embarrassing (and dangerous) breach for the NSA, the world's most advanced signal intelligence agency and best resourced government backed hacking organization. This embarrassment became a muse for the most destructive and fast-spreading ransomware (WannaCry) in History, shutting down hospitals and companies across the Globe. Followed one month later by NotPetya, another highly destructive malware disguised as a ransomware which spread primarily in Ukraine.

Executive Summary

The past 12 months (August 2016 – July 2017) will definitely be remembered as the most active period of the information security industry. Many events have been overlooked due to the high-level activity during this period, although there are numerous events that happened – most of them are related or caused by TheShadowBrokers activity.

- Four public releases, and one private release to a “paid subscriber”.
- Resulted, within months, in offensive capabilities being re-used by global-scale and massively destructive malwares such as WannaCry and NotPetya/Nyeta.
- Release contains tools, anti-forensics utilities to erase logs, finger-printing utilities, local privilege escalation exploits, remote code execution exploits, Command&Control utilities, and kernel mode backdoors.
- Platforms affected so far include embedded devices such as routers but also affect Unix (Linux & Solaris) & Windows desktops and servers.
- Leaks also results the disclosure of hundreds of targets, including Telecom Operators but also extremely detailed information on the compromising of financial institutions such as SWIFT Service Bureaus managing dozens of banks.
- Modus Operandi related documents have also been released containing sensitive information, as part of the metadata of the files, such as the name of the EQUATIONGROUP members who participated and/or led some of those operations.

Details

The emergence of a group like TheShadowBrokers is unprecedented and gives us an inside glance of what the offensive capabilities of EQUATIONGROUP used to be 4 years ago in 2013. As nation state attackers are on the rise, this also give us more information about the general state of art of techniques used by one of the most sophisticated nation-state attacker.

Many events happened since the emergence of TheShadowBrokers, where they have been the common denominator with EQUATIONGROUP of the most recent attacks that happened in the wild.

In August 2016, The Shadow Brokers emerged with a “cyber-weapons auction” which didn’t much traction and led to the free release of several toolkits and exploits. In June 2017, in addition to that, they have also introduced a monthly-based subscription service as a “Cyber Fear as a Service” model where they threatened to release more files and tools belonging to EQUATIONGROUP.

What is the reason for TheShadowBrokers

It is fair to say that over the many month lifespan of TheShadowBrokers the intended purpose of the group has shifted. The earliest releases seem directed towards the Intelligence Community (IC) at a crucial time, probably intended to distract them and divert attention resources towards an internal mole hunt. Later they seem to have been targeting the information security community and threatening former NSA employees, a potentially serious escalation of cyber norms. While the operational role of

TheShadowBrokers has been evolving, the one constant has been their threat to keep releasing stolen EQUATIONGROUP/NSA tools, exploits and data.

TheShadowBrokers presents a credible threat, demonstrating both capability and resolution. They have always followed through by releasing the stolen data, so their resolution is well established. However, they are bounded by a finite resource. Therefore, their capacity is inherently limited and by extension cannot continue for an indefinite period of time.

Finite Data Means Finite Capacity

There is, obviously, a limit to how much stolen data/tools/exploits can be released. There are several impediments to TheShadowBroker releases.

Firstly, they're limited in what they can make public. They've hinted at possessing NSA collected secrets from some countries' nuclear weapons programs – regardless of the veracity of this claim, releasing nuclear weapons program secrets (such as source code or blueprints, etc.) would be a serious breach of multiple treaties. No country would expose itself to those problems. Doubtless there are other treaty protected data sets (e.g. chemical weapons). TheShadowBrokers can only release (presumably) a subset of their stolen data.

Secondly, the data has intelligence value. This value is lost when the data becomes public. Therefore, with each release, it hurts both TheShadowBrokers and the NSA as well. But even barring the obvious intelligence value costs of making a dataset public, TheShadowBrokers still have a problem with finite resources. They can only possess so much of the NSA's full content. Indeed, there is a limit on just how much interesting exploits and tools the NSA possesses.

Given that TheShadowBrokers clearly cannot release stolen NSA exploits indefinitely, and most likely they do not wish to do so. Therefore, one could only speculate and wonder what is to be done?

Recently, TheShadowBrokers announced that they would be releasing new data sets on a monthly subscription basis, a sort of "stolen NSA data of the Month Club". They posted their announcement, set a fixed price, and then provided a Zcash wallet for people to send them crypto-internet-monies. Shortly after they also added a complicated process for paying with Monero, which is a cryptocurrency that offers less privacy from third party inspection.

TheShadowBrokers have made numerous threats to release stolen NSA data for which they have followed through. No one doubts their resolve when it comes to releasing stolen NSA exploits and tools. However, resolve by itself is insufficient to present a credible threat. They need to demonstrate capability. How can they demonstrate this capability?

In January, TheShadowBrokers posted a list of exploits and tools that they threatened to release. NSA's response was swift and decisive – they contacted the vendors and had the underlying vulnerabilities fixed. This "responsible disclosure" was very unlikely done because NSA feels responsible for the software security of civilians, but rather because they are duty bound to deny capability to adversaries.

Lesson learned. Clearly posting lists of stolen exploits leads only to a bug's death. Not a particularly useful outcome. The silent patching doesn't even get any media attention! There is absolutely no upside for TheShadowBrokers via this route.

The problem is simple to state but harder to solve. The ShadowBrokers must demonstrate both **capability to be a credible threat** and **a resolution as well**. Their resolution has already been established. However, they must demonstrate capability (preferably without causing silent bug death). Releasing stolen data from a finite supply means that at some point, they will inevitably lose capability (i.e. run out of data.)

TheShadowBrokers must therefore come up with a plausible infinite stream of stolen data. That the reason for the rise of the "Wine of the Month Club". The data is provided in secret only to subscribers and therefore the quantity, whether it exists, and how much remains are all hidden. The hidden nature of the "Data of the Month Club" is both a strength (disguise how much, if any, EQUATIONGROUP data is dumped) and a weakness (disguise how much, if any, EQUATIONGROUP data is dumped.) A major problem facing TheShadowBrokers is that they lack credibility and only hard proof, the actual data, will convince the intelligence or the information security community.

Timeline

The Timeline



- August 13, 2016 ● TheShadowBrokers Message #1 - Equation Group Cyber Weapons Auction – Invitation
- August 27, 2016 ● F.B.I. raided the home of Harold T. Martin III, an NSA contractor (Booz Allen)
- September, 2016 ● TheShadowBrokers Message#2 - September 2016
- October 1, 2016 ● TheShadowBrokers Message #3
- October 15, 2016 ● TheShadowBrokers Message #4 Bill Clinton/Lynch Conversation
- October 30, 2016 ● TheShadowBrokers Message #5 - TrickOrTreat
- December 14, 2016 ● TheShadowBrokers Message #6 - BLACK FRIDAY / CYBER MONDAY SALE
- January 8, 2017 ● TheShadowBrokers Message #7 - “Windows WareZ”
- January 12, 2017 ● TheShadowBrokers Message#8 – “Farewell Message”
- February 1, 2017 ● Laurent Gaffie drops a Windows SMBv3 0day (non-related to TSB) on GitHub
- February 14, 2017 ● Microsoft delays February Patch Tuesday to March.
- March 14, 2017 ● Microsoft releases MS17-010 which addresses multiple SMB vulnerabilities.
- April 8, 2017 ● TheShadowBrokers Message #8 – “Don’t Forget Your Base” (Medium)
- April 9, 2017 ● TheShadowBrokers migrates previous posts to Steemit.com
- April 9, 2017 (4:58:42 PM PST) ● TheShadowBrokers Message #9 – “Don’t Forget Your Base”
- April 9, 2017 (7:01:36 PM PST) ● TheShadowBrokers Message #10 – “Grammar Critics: Information vs Knowledge”
- April 14, 2017 ● 01.175-10.01.176 version of MeDoc is released with a backdoor.
- April 14, 2017 (1:52:39 AM PST) ● TheShadowBrokers Message #11 – “Lost in Translation”
- May 12, 2017 ● WannaCry ransomware infections starts and infects Windows machines across the Globe.
- May 15, 2017 ● 01.188-10.01.189 version of MeDoc is released with a backdoor.
- May 15, 2017 (11:14:27 PM PST) ● TheShadowBrokers Message #12 – “OH LORDY! Comey Wanna Cry Edition”
- May 29, 2017 (11:06:15 PM PST) ● TheShadowBrokers Message #13 – TheShadowBrokers Monthly Dump Service – June 2017
- June 2nd, 2017 (2:24:03 AM PST) ● TheShadowBrokers Message #14 – TheShadowBrokers Monthly Dump Service - June 2017 Update
- June 22, 2017 ● 01.188-10.01.189 version of MeDoc is released with a backdoor.
- June 27, 2017 (~10:30 AM GMT) - (~3:30AM PST) ● Microsoft MMPC reports telemetry first observation of a Nyeta -related command line.
- June 27, 2017 (11:47:33 PM PST) ● TheShadowBrokers Message #15 – TheShadowBrokers Monthly Dump Service - July 2017
- June 27, 2017 ● Byata/Nyeta/NotPetya ransomware infects most of Ukrainian companies.
- June 31, 2017 (2:45:27 AM PST) ● TheShadowBrokers Message #16 – Response To Response To DOXing
- July 11, 2017 ● TheShadowBrokers are NOT Making America Great again!!!

Wine of the Month Club Timeline

The Timeline



- May 16, 2017 ● Announcement of subscription service
- May 30, 2017 ● zCash wallet posted
- June 1, 2017 ● Monero test@test.com payment
- June 2, 2017 ● Monero wallet posted
- June 27, 2017 ● @fsyourmoms transfers Monero
- July 3, 2017 ● TSB sends a tarball to @fsyourmoms
- July 8, 2017 ● @fsyourmoms Twitter created
- July 11, 2017 ● @fsyourmoms posts TSB is not MAGA
- July 14, 2017 ● @fsyourmoms proves Monero transfer
- July 15, 2017 ● @wh1sks verifies Monero transfer

Timeline Details

August 13, 2016 – Equation Group Cyber Weapons Auction – Invitation

- First appearance, name very likely a reference to the video game: Mass Effect.
- eqgrp-free-file.tar.xz.gpg - Teaser files
- Firewall\{BANANAGLEE, BARGLEE, BLASTING, BUZZDIRECTION, EXPLOITS, OPS, SCRIPTS, TOOLS, TURBO}
 - EGBL = EGREGIOUS BLUNDER (Fortigate Firewall + HTTPD exploit)
 - ELBA = ELIGIBLE BACHELOR
 - ELBO = ELIGIBLE BOMBSHELL (Chinese TOPSEC firewall)
 - ELCA = ELIGIBLE CANDIDATE
 - ELCO = ELIGIBLE CONTESTANT
 - EPBA = EPIC BANANA
 - ESPL = ESCALATE PLOWMAN
 - EXBA = EXTRA BACON (Cisco Adaptive Security Appliance)
 - BANANAGLEE = Juniper Netscreen Devices
 - BARGLEE
 - BLATSTING
 - BUZZDIRECTION
 - SP = ScreamPlow 2.3
 - BD = BananaDaiquiri
- Fortinet, TopSec, Cisco & Juniper firewalls.
- Upload on GitHub by user: userll6gcwaknz@tutanota.com
 - May be a reference to Lelouch Lamperouge VI from Code Geass's anime.
- Asked for 1,000,000 BTC to "Wealthy Elites"
- eqgrp-auction-file.tar.xz.gpg - password protected "CrDj"(;Va.*NdlnzB9M?@K2)#>deB7mN" published Apr 8, 2017.

Name	Size	Type
▶  BANANAGLEE	6 items	Folder
▶  BARGLEE	1 item	Folder
▶  BLATSTING	7 items	Folder
▶  BUZZDIRECTION	2 items	Folder
▶  EXPLOITS	8 items	Folder
▶  OPS	6 items	Folder
▶  SCRIPTS	33 items	Folder
▶  TOOLS	15 items	Folder
▶  TURBO	2 items	Folder

August 27, 2016 – *F.B.I. raided the home of Harold T. Martin III, an NSA contractor working through Booz.*

- "many terabytes of information" according to official reports.

September, 2016 – *TheShadowBrokers Message#2 - September 2016*

- Published additional details on the auction.

October 1, 2016 – *TheShadowBrokers Message #3*

- Q&A on files
- Medium Timestamp: *Sat Oct 01 2016 01:10:40 GMT-0700 (Pacific Daylight Time)*

October 15, 2016 – *TheShadowBrokers Message #4 Bill Clinton/Lynch Conversation*

- "TheShadowBrokers is publicly posting the password when receive 10,000 btc (ten thousand bitcoins)."
- Pastebin Timestamp: *Saturday 15th of October 2016 04:18:43 AM CDT (2:18:43 AM PST)*
- Medium Timestamp: *Sat Oct 15 2016 02:23:10 GMT-0700 (Pacific Daylight Time)*

October 30, 2016 – *TheShadowBrokers Message #5 - TrickOrTreat*

- List of compromised servers and undisclosed tools (DEWDROP, INCISION, JACKLADDER, ORANGUTAN, PATCHICILLIN, RETICULUM, SIDETRACK and STOICSURGEON) related to the operations.
- 306 domains and 352 IP addresses from 49 countries – apparently targeted between 2000 and 2010.
- Mainly Solaris O.S. targets.
- Medium Timestamp: *Sun Oct 30 2016 20:50:53 GMT-0700 (Pacific Daylight Time)*

December 14, 2016 - *TheShadowBrokers Message #6 - BLACK FRIDAY / CYBER MONDAY SALE*

- Direct sales of itemized exploits for individual items priced between 10-100 BTC – and 1,000 BTC for everything.
- One file signed September 1.
- *unix_screenshots.zip*
- Screenshots of files that will later be released on April 8, 2017.

THESHADOWBROKERS ON ZERONET

YOU LIKE. YOU EMAIL. YOU BUY.

Message #6

Download Screenshots (sig)

Name	Type	BTC
auction_file	everything	1,000.0
bs	unknown	10.0
catflap	unknown	10.0
charms	implant	100.0
common	unknown	10.0
curses	implant	100.0
dampcrowd	unknown	10.0
dewdrop	implant	100.0

January 8, 2017 – TheShadowBrokers Message #7 - "Windows Warez"

- New auction for Windows exploits and frameworks.
- Including FUZZBUNCH exploit framework
 - Includes the infamous ETERNALBLUE, ETERNALROMANCE, ETERNALSYNERGY etc.
 - Mentions of a zeroday Windows SMB RCE exploit.
- Including DanderSpritiz
 - Legacy exploits, and tools.
- Total price 750.00 BTC

DanderSpritiz

Name	Type	Price
DanderSpritiz All	DanderSpritiz Everything	250.0 BTC
DanderSpritiz Base	DanderSpritiz LP Only	25.0 BTC

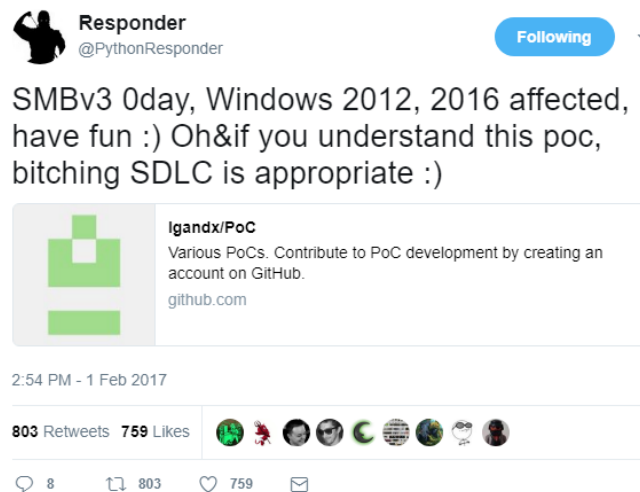
FuzzBunch

Name	Type	Price
FuzzBunch All	FuzzBunch Everything	650.0 BTC
FuzzBunch Base	Exploit Framework only	25.0 BTC
FuzzBunch Exploits	RCEs for IIS, RDP, RPC, SMB	250.0 BTC
FuzzBunch Implants	SMB Cloaked BackDoor	50.0 BTC
FuzzBunch Payloads	Shellcode, Helpers, Tools	50.0 BTC
FuzzBunch Specials	RCE for SMB (Zero Day?)	250.0 BTC
FuzzBunch Storage	BackDoor, Shellcode, Helpers, Tools	50.0 BTC
FuzzBunch Touches	Touches	Free with Exploits

January 12, 2017 – TheShadowBrokers Message#8 – “Farewell Message”

February 1, 2017 – Laurent Gaffie drops a Windows SMBv3 0day (non-related to TSB) on GitHub

- <https://twitter.com/PythonResponder/status/826926681701113861>



February 14, 2017 – Microsoft delays February Patch Tuesday to March.

- Most of the information security researchers’ community thought it was because of Laurent Gaffie’s bug.
- It appears someone may have informed Microsoft about the FUZZBUNCH release teased in January 2017.

March 14, 2017 – Microsoft releases MS17-010 which addresses multiple SMB vulnerabilities.

- Patch includes fixes against ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE and ETERNALSYNERGY exploits released one month later by TheShadowBrokers.
- Other exploits such as EMERALDTHREAD, ERRATICGOPHER, ESIKMOROLL, EDUCATEDSCHOLAR and ECLIPSEDWING have been addresses in prior patches (MS10-061, MS14-068, MS09-050, MS08-067)

April 8, 2017 – TheShadowBrokers Message #8 – “Don’t Forget Your Base” (Medium)

- Medium Timestamp: Sat Apr 08 2017 04:05:16 GMT-0700 (Pacific Daylight Time)

April 9, 2017 – TheShadowBrokers migrates previous posts to Steemit.com

- Message #1 @ 4/9/2017, 3:38:57 PM PST
- Message #2 @ 4/9/2017, 3:44:54 PM PST
- Message #3 @ 4/9/2017, 3:58:54 PM PST
- Message #4 @ 4/9/2017, 4:05:21 PM PST
- Message #5 @ 4/9/2017, 4:15:27 PM PST
- Message #6 @ 4/9/2017, 4:25:33 PM PST

- Message #7 @ 4/9/2017, 4:37:18 PM PST
- Message #8 @ 4/9/2017, 4:53:21 PM PST

April 9, 2017 (4:58:42 PM PST) – TheShadowBrokers Message #9 – “Don’t Forget Your Base”

- “The password for the EQGRP-Auction-Files is CrDj”(;Va.*NdlnzB9M?@K2)#>deB7mN”
- rpc.cmsd - Remote root zero-day exploit for Solaris
- TOAST Framework – No Logs No Crime – Clear wtmp log events
- ELECTRICSLIDE – Fake Chinese metadata
- Several Remote Code Executions for Solaris, Netscape Server, FTP Servers, Web CMS, Mail Servers, Web Servers, Printers, etc.
- Several anti-forensics tools to erase logs post operations (TOAST, PCLEANS, DIZZYTACHOMETER, DUBMOAT, SCRUBHANDS, AUDITCLEANER)
- Several remote access tools, and command and control for HP-UX, Linux and SunOS.
- Several privilege escalations for Linux and AIX
- Some extract of operations notes on 11 targets – most likely all mobile operators (SICKLESTAR, EDITIONHAZE, SILENTTONGUES, SICKLESTAR, LIQUIDSTEEL, SERENECOSMOS, WHOLEBLUE, DIAMONDAXE, SHAKENGIRAFFE, DARKAXE, COASTALSTORM)
 - PITCHIMPAIR also released as part of the leak.
- Medium Timestamp: Sat Apr 08 2017 04:05:16 GMT-0700 (Pacific Daylight Time)

April 9, 2017 (7:01:36 PM PST) – TheShadowBrokers Message #10 – “Grammer Critics: Information vs Knowledge”

- Responds to critics claiming the broken English is too fake to be true.

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

- Reported by Cisco Talos Team.

April 14, 2017 (1:52:39 AM PST) – TheShadowBrokers Message #11 – “Lost in Translation”

- *“This week theshadowbrokers be thinking fuck peoples.”*
- Drops “Windows Warez” dump (windows.tar.xz.gpg) from January 8, 2017 auction which includes FUZZBUNCH exploitation framework, multiple Windows exploits such as ETERNAL* exploits, and utilities such as PASSFREELY which does in memory patching of the Oracle database authentication routines to allow any connections.
- Includes an archive (swift.tar.xz.gpg) containing highly detailed operational notes proving the EquationGroup had targeted and gained access to the servers of a SWIFT Service Bureau in Middle East which operates multiple banks across the region.
 - Contains unredacted metadata, including PowerPoint presentations, modus operandi description and tools used at different steps

- Contains SQL script which had been used during the operation to dump the SWIFT messages from the database.
- Includes ODDJOB (*odd.tar.xz.gpg*) an implant builder and C2 server.

May 12, 2017 – WannaCry ransomware infections starts and infects Windows machines across the Globe.

- 150 countries affected within the first days.
 - Victim includes worldwide banks, government entities and hospitals.
- Multiple variants deployed within the first 7 days of the infection.
 - May 12, 2017 - First kill-switch registered by KryptosLogic.
 - May 14, 2017 - Second kill-switch registered by Comae Technologies.
 - Comae's Team still receive signals of activity of this variant.
 - More than 1M hits received and infection prevented by Comae between May 2017 and July 2017.
 - This variant is still active, and suggests the other ones are too.
- WannaCry made ETERNALBLUE exploit World famous, as it was leveraging it on both the internal and external networks.

May 15, 2017 – 01.188-10.01.189 version of MeDoc is released with a backdoor.

- Reported by Cisco Talos Team.

May 15, 2017 (11:14:27 PM PST) – TheShadowBrokers Message #12 – “OH LORDY! Comey Wanna Cry Edition”

- Non-apology apology from TheShadowBrokers to have released exploits that have been used by WannaCry to spread.
- First announcement of a monthly-based subscriptions subtitled “Wine of the Month Club”, where TSB claims to have:
 - Most recent files than the exploits and tools that have been leaked so far (latest files are 2013 timestamped)
 - New targets such as Web Browsers, Routers or even Windows 10 exploits.
 - More operational notes on SWIFT providers and Central Banks. Initial proof and modus operandi of such attacks have been initially disclosed by TSB one month before.
 - Compromised network data from Russian, Chinese, Iranian and North Korean nukes and missile programs.

May 29, 2017 (11:06:15 PM PST) – TheShadowBrokers Message #13 – TheShadowBrokers Monthly Dump Service – June 2017

- Discloses initial payment details for June's release.

- Monthly fee for a monthly subscription.
- Asks for 100 ZEC (Zcash) for dump.

June 2nd, 2017 (2:24:03 AM PST) - TheShadowBrokers Message #14 – TheShadowBrokers Monthly Dump Service - June 2017 Update

- Announcement of a new method of payment (Monero)
- Asks for 500 XMR as an alternative to Zcash for June's subscription.

June 22, 2017 – 01.188-10.01.189 version of MeDoc is released with a backdoor.

- Reported by Cisco Talos Team

June 27, 2017 (~10:30 AM. GMT) - (~3:30AM PST) – Microsoft MMPC reports telemetry first observation of a Nyeta -related command line.

- *"We observed telemetry showing the MEDoc software updater process (EzVit.exe) executing a malicious command-line matching this exact attack pattern" – Microsoft MMPC*

June 27, 2017 (11:47:33 PM PST) - TheShadowBrokers Message #15 – TheShadowBrokers Monthly Dump Service - July 2017

- 200 ZEC or 1000 XMR for July dump.
- Claims it received mystery gift from unknown people and posts a link.
- Threatens to reveal the identity of additional former equation group members.

June 27, 2017 – Byata/Nyeta/NotPetya ransomware infects most of Ukrainian companies.

- The ransomware deployed itself through a rogue update from a Ukrainian tax accounting software MeDoc
- Infects local network of MeDoc software users by leveraging both mimikatz and ETERNALBLUE
- Primarily targets Ukrainian companies and government entities.

June 31, 2017 (2:45:27 AM PST) - TheShadowBrokers Message #16 – Response To Response To DOXing

- Responds to Twitter trolls.

July 11, 2017 - TheShadowBrokers are NOT Making America Great again!!!

- Unhappy "Wine of the Month Club" customer (@fsyourmoms) complained that TSB only sent a single tool and no exploit.
- User later posted a proof of email received on the July 3, 2017 about the private release.
- User email is the same as the GitHub email used in August 2016.
- @fsyourmoms may be a character created only to assist TSB to maintain credibility.
 - Still unclear how TSB was able to email on an external domain without having pre-shared a password with @fsyourmoms

- Tutanota requires a pre-shared key if a Tutanota emails an external domain.

 Tutanota®

This version of Tutanota is a service for private users.

Sign up

Logout

Edit

Inbox

Drafts

Sent

Trash

Archive

Spam

June Subscription

userl6gcwknz@tutanota.com

07:26

From userl6gcwknz@tutanota.com

To Me <fucksyourmoms@protonmail.com>

June Subscription

june.tar.xz.gpg (2 MB) june.tar.xz.gpg.sig (542 B)

Thank you for subscribing.

The June file is attached.

The password is dQb9^:M.1yT0n.fn)FOe!RZ&

TSB hope you will subscribe again in July.

--

Securely sent with Tutanota. Claim your encrypted mailbox today!
<https://tutanota.com>

Reply confidentially

Move

Delete

Mo 3. Jul 07:26

Conclusion

Unfortunately, we don't foresee any reasons to slow down the events for the second parts of both 2017 and 2018. We recommend companies and government entities to be alert. The past 12 months have showed us an entirely new level of complex attacks. Such attacks originating from non-ordinary attackers' hits IT Administrators hard and leaves them not knowing anything had even happened. Needless to say, they are not prepared for such sophisticated and complex attacks, compared to the common ones they are used to seeing most of the time. Having witnessing all that in public and seeing real case scenarios of such information being leveraged and abused by cyber-criminals leaves us with only one conclusion, which is that highly orchestrated attacks leveraging highly sophisticated exploits such as remote kernel code executions and backdooring legitimate products through supply-chain attacks are a reality and some conspiracy theories one would speculate.

TheShadowBrokers have threatened to release exploits, tools and utilities targeting more platforms including recent ones through their monthly subscription. At the moment, the June monthly release appeared to have been a single tool. However, it is safe to assume that TheShadowBrokers probably have more compromising information on the practice of the Intelligence Community, but also more exploits and tools that could be future threats.

Ransomware infection is obvious due to its damaging nature and the fact that it affects the production of companies and individuals. Moreover, it is highly likely that those tools and exploits are being used for exfiltration purposes by criminals without being detected. Until now, most of the coverage was done on the Windows exploits but the Unix exploits are as damaging and as relevant as well.

It is still unclear if WannaCry, NotPetya and TheShadowBrokers are dissociative or associative groups as both the identity and the intent of the attackers still remains largely unknown and confusing for most part.

Until now, the most recent exploits and tools were dated from 2013 – this also means that there is a high probability that further criminal groups and nation state attackers have had access to and developed more sophisticated arsenal over the past four years.

Operating Systems (O.S.) vendors such as Microsoft have been raising the bar for exploitation with several mitigations as part of Windows 10 and the upcoming Redstone 3 (Windows 10 Fall Creators Update). We expect more vendors to do the same. Since, threats are difficult for third party products mitigate as they are not integrated within the OS itself, but rather as a secondary layer of defense.

From a policy point of view, this shows how inefficient arrangements such as Wassenaar Arrangement not only to the parties who failed to contain and keep control of such tools, but also, that the laws of software and digital data don't apply the same way as more traditional weapons. The total exact cost of damage from breaches like WannaCry and NotPetya still remains unknown. However, estimated figures are in billions of dollars. Despite having joint effort from the information security community and response help to mitigate further propagation, it was often too late in many cases.

We urge companies to prepare incident response and recovery plans, in anticipation of more sophisticated, invasive or destructive attacks like the ones we have seen and covered in this paper.

THIS PAGE IS INTENTIONALLY LEFT BLANK



comae
technologies

Comae Technologies is a cybersecurity company
founded in 2016.

Don't be the last one to know about your own
breach.

info@comae.io
www.comae.io