



JULY 22-27, 2017
MANDALAY BAY / LAS VEGAS

The Shadow Brokers Cyber Fear Game-Changers

Matt Suiche (@msuiche)



 #BHUSA / @BLACKHATEVENTS

Who am I?

theshadowbrokers

@shadowbrokerss

Following



Replying to [@cypherseek](#) [@msuiche](#)

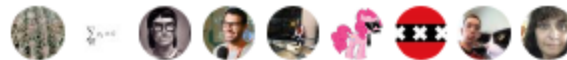
sarcasm? don't be mean to [@msuiche](#) he looks like such fun guy, is one thing to be hacker smart is another to be entrepreneur, but to be both

Retweets

7

Likes

7



11:30 PM - 29 May 2017



2



7



7



Who am I?

- French Reverse-Engineer
- Founder of Comae Technologies
 - Cybersecurity startup
 - Deep Dive Incident Response Platform
 - Threat Intelligence
- Co-Founder of CloudVolumes (VMware)
- @msuiche / m@comae.io

Who are *(is?)* TheShadowBrokers?

theshadowbrokers

@shadowbrokerss

Following



Replying to @drwolfff @msuiche

What is a TAO? TSB is not buddists

Retweets

6

Likes

10



12:17 AM - 30 May 2017



2



6



10



Multiple Theories

- Group versus Individual
 - The Shadow Brokers versus TheShadowBrokers
- Angry Insider
 - Tim Shorrock highlighted the Intelligence Community hires around **45,000** contractors.
 - Angry
 - Exposed the identity of agents and the language.
 - Insider
 - Showed deep knowledge of the organization numerous times.
 - File hierarchy intact.
- Someone who got access to files stolen by a contractor which exposed them ?
- Hacked server
 - This was one of the initial theory but this one doesn't make sense at all now.
 - Mainly due to the operational notes leaked.

Cyber Fear As A Service (CFaaS)

- TheShadowBrokers first emerged on August 13, 2016
 - Name very likely inspired from video game Mass Effect
- Asked for 1,000,000 BTC
- GitHub user: userll6gcwaknz@tutanota.com
 - Potential reference to Lelouch Lamperouge VI from Code Geass's anime.
 - *Former prince Lelouch vi Britannia obtains a power known as Geass and decides to use it to obliterate the Holy Britannian Empire, a superpower that has been conquering various countries.*
 - Email used again on July 3, 2017 to one of the "Subscription Member"
- Twitter user: @shadowbrokerss
- Steemit user: @theshadowbrokers

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 – “Grammer 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!!!

Equation Group Cyber Weapons Auction Invitation

August 13, 2016

- Free samples containing Firewall appliances exploits.
 - Fortigate Firewall
 - Chinese TOPSEC firewall
 - Cisco Adaptive Security Appliance
 - Juniper Netscreen Devices
- [eqgrp-free-file.tar.xz.gpg](#)
- [eqgrp-auction-file.tar.xz.gpg](#)
 - Password protected archive
 - Password published in April 2017

eqgrp-free-file.tar.xz.gpg

- 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

August 27, 2016

- FBI raids the home of Harold T. Martin III, an NSA contractor working for Booz Allen
- "many terabytes of information" according to official reports.

Former Booz Allen Hamilton contractor Harold Thomas Martin III allegedly stole secret and top-secret software and documents from American intelligence agencies for up to 20 years. That's according to a federal grand jury indictment revealed today.

"The indictment alleges that beginning no earlier than 1996 and continuing through August 27, 2016, Martin stole and retained US government property, including documents that bore markings indicating that they were property of the US and contained highly classified information, including TOP SECRET/SCI. A Top Secret classification means that unauthorized disclosure reasonably could be expected to cause exceptionally grave damage to the national security of the US.

The Uprising

September, 2016

- *TheShadowBrokers Message#2 - September 2016*

October 1, 2016

- *TheShadowBrokers Message #3*
- Q&A

October 15, 2016

- *TheShadowBrokers Message #4 Bill Clinton/Lynch Conversation*
- Asks for 10,000 BTC to publish the password

October 30, 2016

- List of compromised servers and undisclosed tools related to the operations.
 - DEWDROP, INCISION, JACKLADDER, ORANGUTAN, PATCHICILLIN, RETICULUM, SIDETRACK and STOICSURGEON
- 306 domains and 352 IP addresses from 49 countries – apparently targeted between 2000 and 2010.
- Mainly Solaris O.S. targets.

December 14, 2016

- Direct sales of itemized exploits for individual items priced between 10-100 BTC – and 1,000 BTC for everything.
- One file signed September 1.
- Preview of August archive

[THESHADOWBROKERS.BIT](#)
[LISTOPWAREZ](#) [MESSAGES](#) [CONTACT](#)

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

Message #7 - "Windows Warez"

January 8, 2017

- 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 DanderSpritz
 - Legacy exploits, and tools.
- Total price 750.00 BTC

DanderSpritz

Name	Type	Price
DanderSpritz All	DanderSpritz Everything	250.0 BTC
DanderSpritz Base	DanderSpritz 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

TheShadowBrokers Message#8 – “Farewell Message”

January 12, 2017

- Farewell Message
 - TSB expresses disappointment due to the fact nobody seriously participated in the auction.
 - Never Say Never

February 1, 2017

- *Security Researcher, Laurent Gaffie drops a Windows SMBv3 0day (non-related to TS*



Responder
@PythonResponder

Following

SMBv3 0day, Windows 2012, 2016 affected,
have fun :) Oh&if you understand this poc,
bitching SDLC is appropriate :)



Igandx/PoC

Various PoCs. Contribute to PoC development by creating an
account on GitHub.

github.com

2:54 PM - 1 Feb 2017

803 Retweets 759 Likes



8



803



759



Patch Tuesday Delayed

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.
 - Is it ? Was it ? Thanks to Laurent anyway !
- It appears someone may have informed Microsoft about the FUZZBUNCH teaser from January 2017.

March 14, 2017

- Microsoft releases MS17-010 which addresses multiple SMB vulnerabilities.
 - Patch also includes fixes against ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE and ETERNALSYNERGY exploits released one month later by TheShadowBrokers

Message #8 – “Don’t Forget Your Base”

April 8, 2017

- Medium blogpost – Also a second Tuesday of the month

April 9, 2017

- Migrates to Steemit
 - Blogging platform powered by a blockchain database
- TSB drops the password of the August 2016 archive.
 - “The password for the EQGRP-Auction-Files is
CrDj”(;Va.*NdlnzB9M?@K2)#>deB7mN”

EQGRP-Auction-Files (1/2)

- Very significant dump which had been mainly overlooked so far.
- 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)

EQGRP-Auction-Files (2/2)

- 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 – very likely all mobile operators (**SICKLESTAR**, EDITIONHAZE, SILENTTONGUES, SICKLESTAR, LIQUIDSTEEL, SERENECOSMOS, WHOLEBLUE, DIAMONDAXE, SHAKENGIRAFFE, DARKAXE, COASTALSTORM)
 - PITCHIMPAIR also released as part of the leak.

Message #10 – “Grammer Critics: Information vs Knowledge”

- Responds to critics claiming the broken English is too fake to be true.
 - *The ShadowBrokers is writing TRADOC, Position Pieces, White Papers, Wiki pages, etc for USG. If theshadowbrokers be using own voices, theshadowbrokers be writing peoples from prison or dead. TheShadowBrokers is practicing obfuscation as part of operational security (OPSEC).*

Message #11 – “Lost in Translation”

April 14, 2017 (1:52:39 AM PST)

- “This week theshadowbrokers be thinking fuck peoples.”
- windows.tar.xz.gpg
 - “Windows Warez” initially teased in January
 - FUZZBUNCH, ETERNAL* (SMB remote exploits) and PASSFREELY
- swift.tar.xz.gpg
 - Very detailed operational notes proving EQGRP sought and gained access to the backbone of international financial system to have a God’s eye into a SWIFT Service Bureau.
 - Why not just asking for it ?
 - SQL script to dump SWIFT messages from the Oracle database
- odd.tar.xz.gpg
 - *Implant builder*

- Can be deployed remotely
 - DOUBLEPULSAR
- 386 variants of Oracle server.
- Only patches 4 bytes in memory
 - Bypasses authentication for servers

```
lpBaseAddress = va;
if ( !VirtualProtectEx(hProcess, va, 4u, 0x40u, &flOldProtect) )
    return 12;
ReadProcessMemory(hProcess, va, &readMemValue, 4u, &NumberOfBytesRead);
if ( NumberOfBytesRead != 4 )
    return 13;
dwXOR = oracleEntry[6];
dwOrigin = oracleEntry[2];
dwModified = oracleEntry[4];
dwXOR2 = oracleEntry[6];
if ( cchMultiByte )
{
    snprintf(
        &MultiByteStr,
        0x100u,
        "\t%s %8x, %s %8x, %s %8x, %s %8x\n",
        &Orig_str,
        dwOrigin,
        &Modified_str,
        dwModified,
        &XOR_str,
        dwXOR,
        &MemValue_str,
        readMemValue);
    convertString(cchMultiByte, &MultiByteStr);
}
if ( (readMemValue != dwOrigin || !a3) && (readMemValue != dwModified || a3) )
    break;
if ( enablePatch )
{
    readMemValue ^= dwXOR2;
    WriteProcessMemory(hProcess, lpBaseAddress, &readMemValue, 4u, &NumberOfBytesWritten);
    if ( NumberOfBytesWritten != 4 )
        return 14;
}
if ( !VirtualProtectEx(hProcess, lpBaseAddress, 4u, flOldProtect, &v17) )
    return 16;
```

```

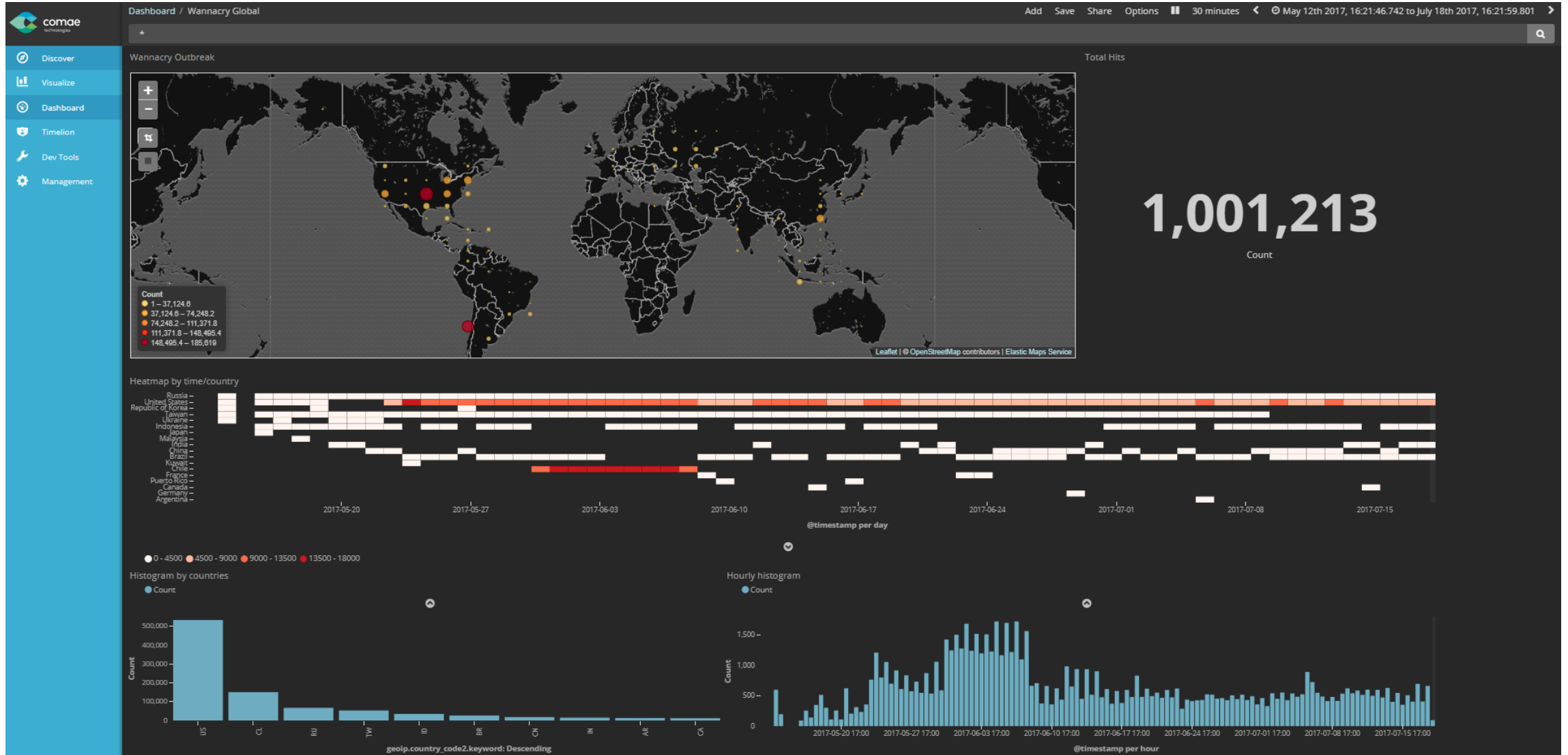
11 prompt
12 set termout off
13 spool d41af8c_a.tmp
14 select 'set long 4096' from dual;
15 select 'set lines 1024' from dual;
16 select 'set longc 4096' from dual;
17 select 'set wrap on' from dual;
18 select 'set recsep off' from dual;
19 select 'set pages 0' from dual;
20 select 'set feedback off' from dual;
21 select 'set verify off' from dual;
22 select 'set trimspool on' from dual;
23 select 'spool &&output_file_name append' from dual;
24 select 'select '''SENDER_CC","RECEIVER_CC","MESG_S_UMID","SWIFT_MESSAGE''' from dual;' from dual;
25 select 'select '''||substr(mesg_sender_swift_address,5,2)||''','''||substr(mesg_receiver_swift_address,5,2)||''','''||mesg_s_umid||''','''||
26 ltrim((select to_char(appe_session_nbr,'0000')||ltrim(to_char(appe_sequence_nbr,'000000'))
27 from saaowner.appe_||substr(table_name,6,20)||' a
28 where a.appe_s_umid = m.mesg_s_umid and a.appe_iapp_name = 'SWIFT' and rownum = 1)) ||
29 ''')'||''{2:''||decode(substr(m.mesg_uumid,1,1),'0','0')||mesg_type||
30 ltrim((select to_char(TO_DATE (((TO_NUMBER (TO_CHAR (TO_DATE ('1970-01-01 00:00:00', 'yyyy-mm-dd hh24:mi:ss'), 'J'), '99999999
31 ((appe_remote_input_time - (MOD (appe_remote_input_time, 86400))) / 86400)), 'J') +
32 ((MOD (appe_remote_input_time, 86400)) / 86400),'hh24mi')||appe_remote_input_reference||
33 to_char(TO_DATE (((TO_NUMBER (TO_CHAR (TO_DATE ('1970-01-01 00:00:00', 'yyyy-mm-dd hh24:mi:ss'), 'J'), '99999999')) +
34 ((appe_local_output_time - (MOD (appe_local_output_time, 86400))) / 86400)), 'J') +
35 ((MOD (appe_local_output_time, 86400)) / 86400),'yymmddhh24mi')
36 from saaowner.appe_||substr(table_name,6,20)||' a
37 where a.appe_s_umid = m.mesg_s_umid and a.appe_iapp_name = 'SWIFT' and rownum = 1))
38 ||decode(m.mesg_network_priority,1,'S',2,'U',3,'N','N'),'I','I')||mesg_type||
39 mesg_receiver_swift_address||decode(m.mesg_network_priority,1,'S',2,'U',3,'N','N')
40 , 'OTHER')||''{3:''||text_swift_block_3||
41 ''}{4:''||text_data_block||''
42 -){5:''||utl_raw.cast_to_varchar2(dbms_lob.substr(text_swift_block_5))||''}''' SWIFT_MESSAGE
43 from saaowner.text_||substr(table_name,6,20)||' t ,saaowner.mesg_||substr(table_name,6,20)||' m
44 where
45 m.mesg_s_umid = t.text_s_umid and
46 text_swift_block_5 is not null;'||'
47 spool off
48 set termout on
49 prompt date '''||substr(table_name,6,8)||' completed.
50 set termout off
51 spool '&&output_file_name' append'

```

May 12, 2017

- 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.

WannaCry is still active



Message #12 – “OH LORDY! Comey Wanna Cry Edition”

May 15, 2017 (11:14:27 PM PST)

- 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:
 - Files more recent than the exploits and tools
 - latest files are 2013 timestamped so far.
 - New targets
 - Web Browsers, Routers or even Windows 10 exploits.
 - More operational notes on SWIFT providers and Central Banks.
 - Compromised network data
 - Russian, Chinese, Iranian and North Korean nukes and missile programs.

Message #13 – TheShadowBrokers Monthly Dump Service – June 2017

- Wine of the Month Club
 - Cyber-Fear as a Service
- Discloses initial payment details for June's release.
 - 100 ZEC (Zcash) for June
 - 500 XMR (Zcash alternative – Message #14)
- No information on the release

NotPetya/Nyeta/Byata

June 27, 2017 (~10:30 AM. GMT) - (~3:30AM PST)

- *"We observed telemetry showing the MEDoc software updater process (EzVit.exe) executing a malicious command-line matching this exact attack pattern" – Microsoft MMPC*
- *Leverages ETERNALBLUE locally if credential in memory robbery fails.*

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.

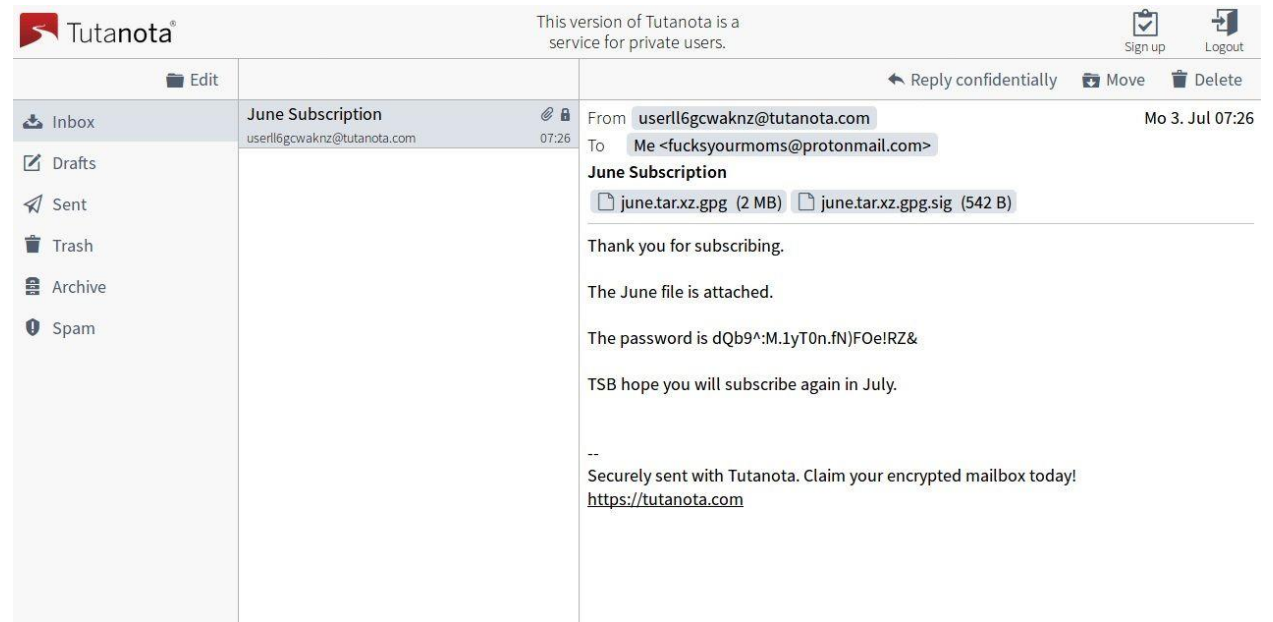
Message #16 – Response To Response To DOXing

June 31, 2017 (2:45:27 AM PST)

- Responds to Twitter trolls.

July 11, 2017

- Unhappy client complains about June's wine selection
- Claims to have receive only a single tool
- User later posted a proof of email received on the July 3, 2017 about the private release
- userll6gcwaknz



Wine of The Month

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

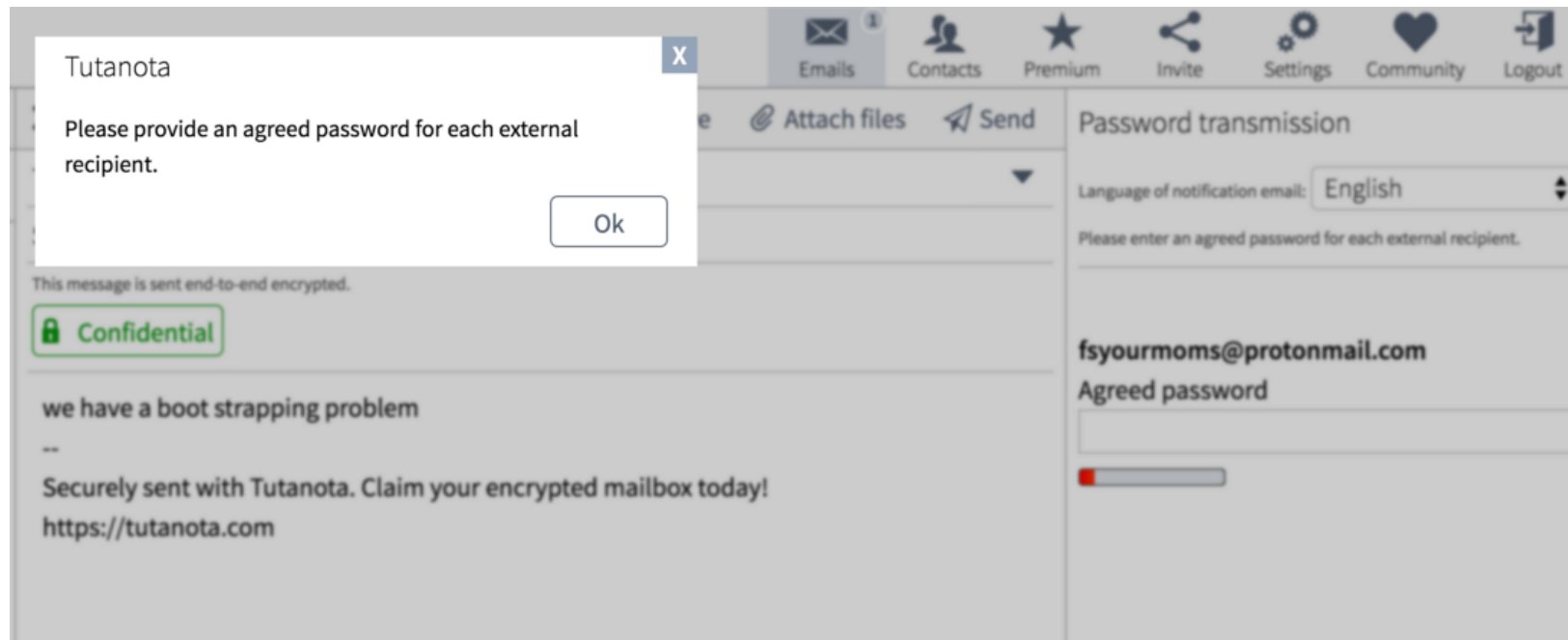
- Medium: @fsyourmoms / Email: fucksyourmoms@protonmail.com
- May be a character created by TSB to maintain credibility.

Is theshadowbrokers doing correct? If not theshadowbrokers is sure many haters be posting smart comments. Is being ok, theshadowbrokers fucks your moms. You getting idea.

- Buyer can cryptographically prove that a transfer had been made
 - a944723f77415dd06c5d34260363935e24ac6d5ac7fe711366f64768fa055803
 - But Monero has a privacy layer, it can *only* prove a transaction had been made. Not its details.
 - May explain why TSB moved from Zcash to Monero ?
- Is @fsyourmoms a fabricated "trusted third party" ?

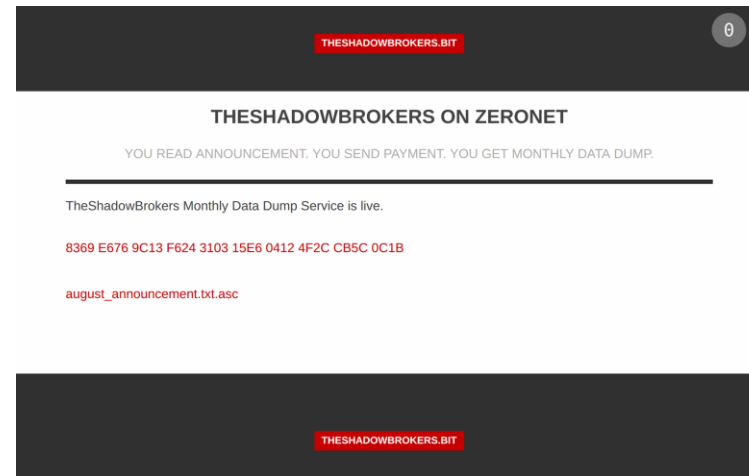
Pre-Shared Key Mystery ?

- Tutanota can't email external domain (protonmail.com) without exchanging a pre-shared password.
- How did they exchanged it ?



Monthly Service - August 2017

- 6 hours ago.
- 500 ZEC / 2000 XMR
 - Pricing keeps doubling.
 - Less and less guarantee of having more files.
- zvg3gyomywniv8@zeroid.bit / bimigjt3xne0@mail.i2p
- *"July data dump for subscribers inbound. Interesting June data dump not published by subscribers."*





 · 37 · 3 hours ago

That's very interesting! Thank you @theshadowbrokers!

 \$0.00 | Reply



 · 37 · 3 hours ago

it looking good but i dont think i will be legal

upvote

 \$0.00 | Reply

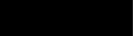


 · 27 · 2 hours ago

Good post man. Thanks!

 \$0.00 | Reply



 · 58 · 1 hour ago

Interesting information. Thank you.

 \$0.00 | Reply

Conclusion

- Wassenaar Arrangement proved inefficient
- Who is responsible ? Shared responsibility ?
 - Although, kudos to Microsoft for quickly improving and adding security mitigation scene so quickly (cf. Windows 10 RS3)
 - What about less secure platforms ? IoTs, Solaris etc.
 - Should the IC share vulnerabilities with vendors ?
 - Backdoor debate ?
- Small Medium Businesses are prime victims
 - Often unprepared (no defense, legacy infrastructure, no IR or recovery plan)
- Attacks significantly more sophisticated
- Rising threat from unreliable IC employees ☹️

m@comae.io / @msuiche

References

- <https://www.washingtonpost.com/posteverything/wp/2017/03/16/the-reason-wikileaks-receives-so-many-u-s-state-secrets-private-contractors/>
- <https://blog.comae.io/theshadowbrokers>
- <https://blog.comae.io/wannacry>
- <https://blog.talosintelligence.com/2017/07/the-medoc-connection.html>
- <https://blog.comae.io/byata>