TheShadowBrokers

One year later…

SANS Prague (1st October 2018)

Matt Suiche

Founder, Comae Technologies

msuiche@comae.com
@msuiche

Who am I? - @msuiche

- Comae Technologies *(www.comae.com)*
  - Comprehensive Memory Forensics Platform
    - Stardust
  - Memory acquisition tool that works
    - DumpIt
    - Formerly called win32dd, exists since 2008 (10 Years!)
- OPCDE *(www.opcde.com)*
  - Operation Community Development & Empowerment
  - Cybersecurity conference in Dubai, UAE & Nairobi, Kenya
  - Always looking for sponsors/patrons!
- “a fun guy” according to TheShadowBrokers

Attribution can be confusing...

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 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 infection 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 11:13:27 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 2, 2017 2:24:03 AM PST	TheShadowBrokers Message #13 – TheShadowBrokers Monthly Dump Service – June 2017 - Update
June 27, 2017 -10:30 AM GMT – 2:24:03 AM PST	Microsoft MMPC reports telemetry first observation of Nyeta related command
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 American Great again!!!
July 27, 2017	TheShadowBrokers Monthly Dump Service - August 2017
September 6, 2017 10:11 AM PST	TheShadowBrokers Dump Service - September 2017
October 16, 2017	TheShadowBrokers - October Price Adjustment
December 1, 2017	Nghia Hoang Pho, former NSA TAO employee, pleaded guilty to willful retention of national defense information.
December 13, 2017	Trump signs into law U.S. government ban on Kaspersky Lab software.
September 24, 2018	Nghia Hoang Pho, 68, is sentenced to 5.5 years for storing classified information at home.
October 31, 2018	Halloween 2018? TSB claimed in a response that Halloween is his favorite holiday.

Nothing in 2017... Halloween 2018?

Hello Matt Suiche,

TheShadowBrokers is sorry TheShadowBrokers is missing you at theblackhats or maybe not? TSB is not seeing hot reporter lady giving @msuiche talk, was that not being clear required condition? TheShadowBrokers is being sures you understanding, law enforcements, not being friendly fans of TSB. Maybe someday. Dude? "...@shadowbrokerss does not do thanksgiving. TSB is the real Infosec Santa Claus..." really? "Trick or Treet", cosplay and scarring shits out of thepeoples? TheShadowBrokers favorite holiday, not holiday, but should be being, Halloween!

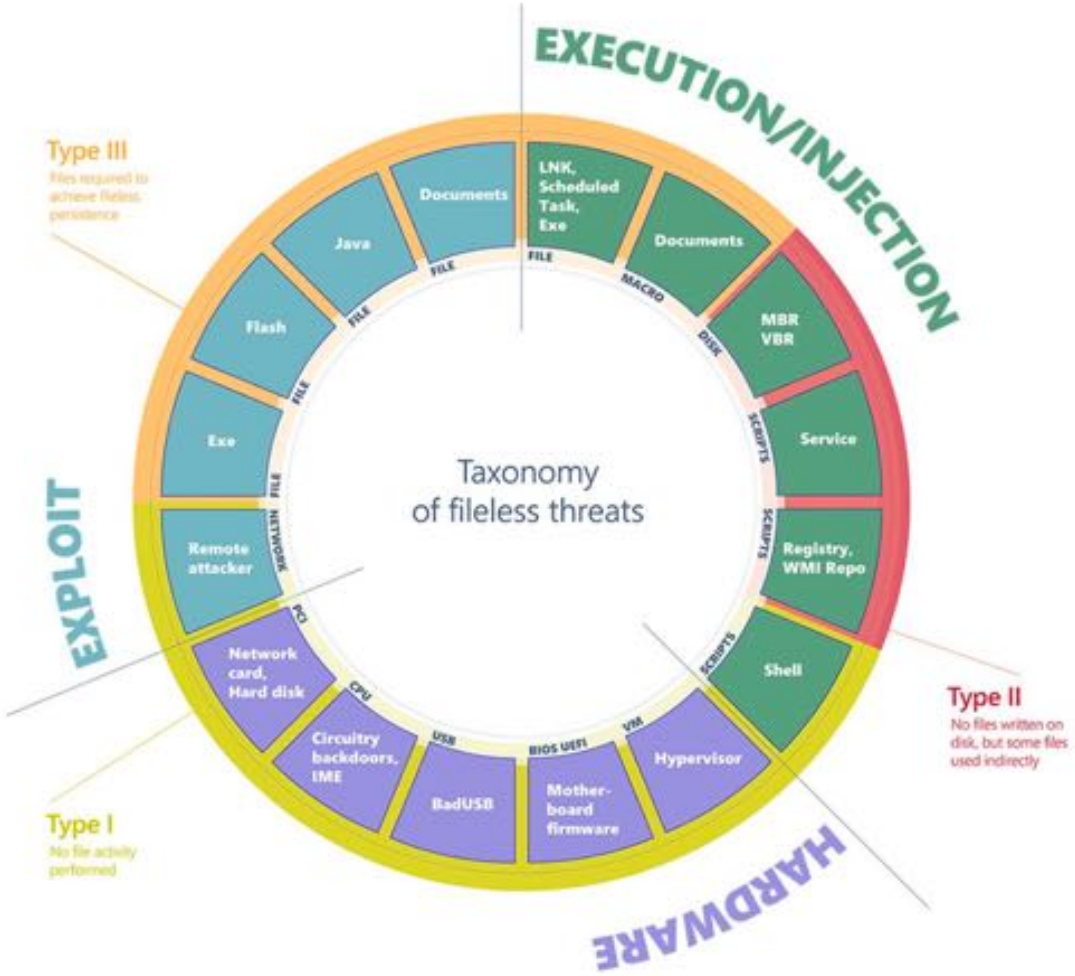
Most controversial release

- The SWIFT Service Bureau toolchain
  - Operational notes
  - MS17-010 exploits (ETERNALBLUE, etc..)
    - Repackaged by WannaCry & NotPetya
  - DOUBLEPULSAR backdoor
  - https://blog.comae.io/the-nsa-compromised-swift-network-50ec3000b195
- Those exploits are 5 years old, have been public for one year but their internals are still a hot discussion topic.
  - DerbyCon (October 2018) – zerosum0x0 - MS17-010?
  - DEFCON 26 – zerosum0x0 – Eternal Exploits

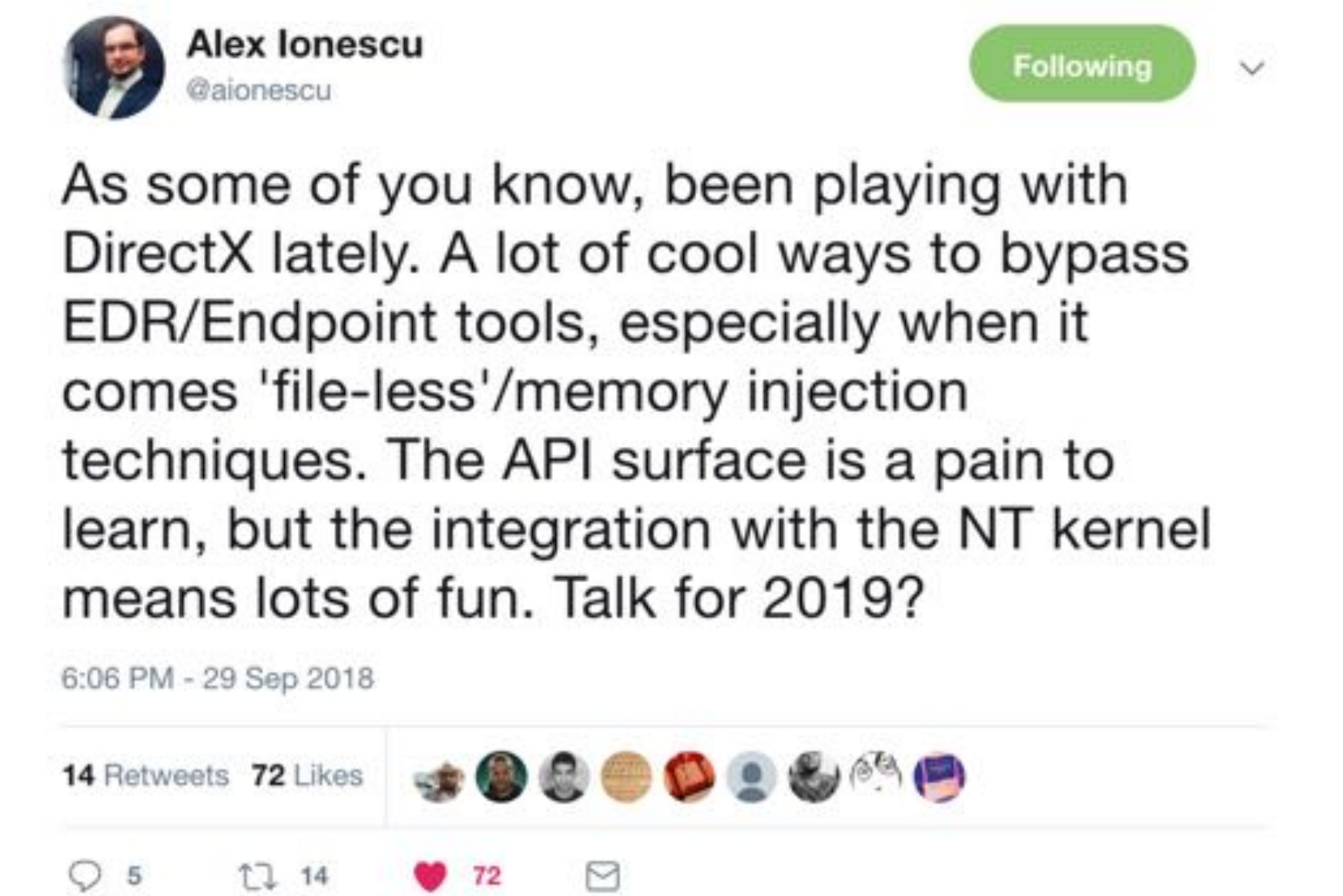
Post-MS17-010 for Incident Responders

- was just a déjà vu of MS10-061 , MS09-050, MS08-067… Did we get better?
- Patching + System Hardening is import.
  - Enterprise are moving towards newer systems.
- What does that mean for incident responders?
  - Your tools need to be up-to-date!
  - Got 99 problems but Vista ain't one. No support for RS5+ won't do any good to Incident Responders.
- DOUBLEPULSAR backdoor, fileless malwares…
  - How do you detect that?
  - EDR etc. solutions are improving but they are runtime. Intel even came up with Intel AMS (Advanced Memory Scanner)
  - But how do you perform offline analysis which is often required for Incident Response?

Fileless Threats



Out of sight but not invisible: Defeating fileless malware with behavior monitoring, AMSI, and next-gen AV.
Windows Defender Research (September 28, 2018)

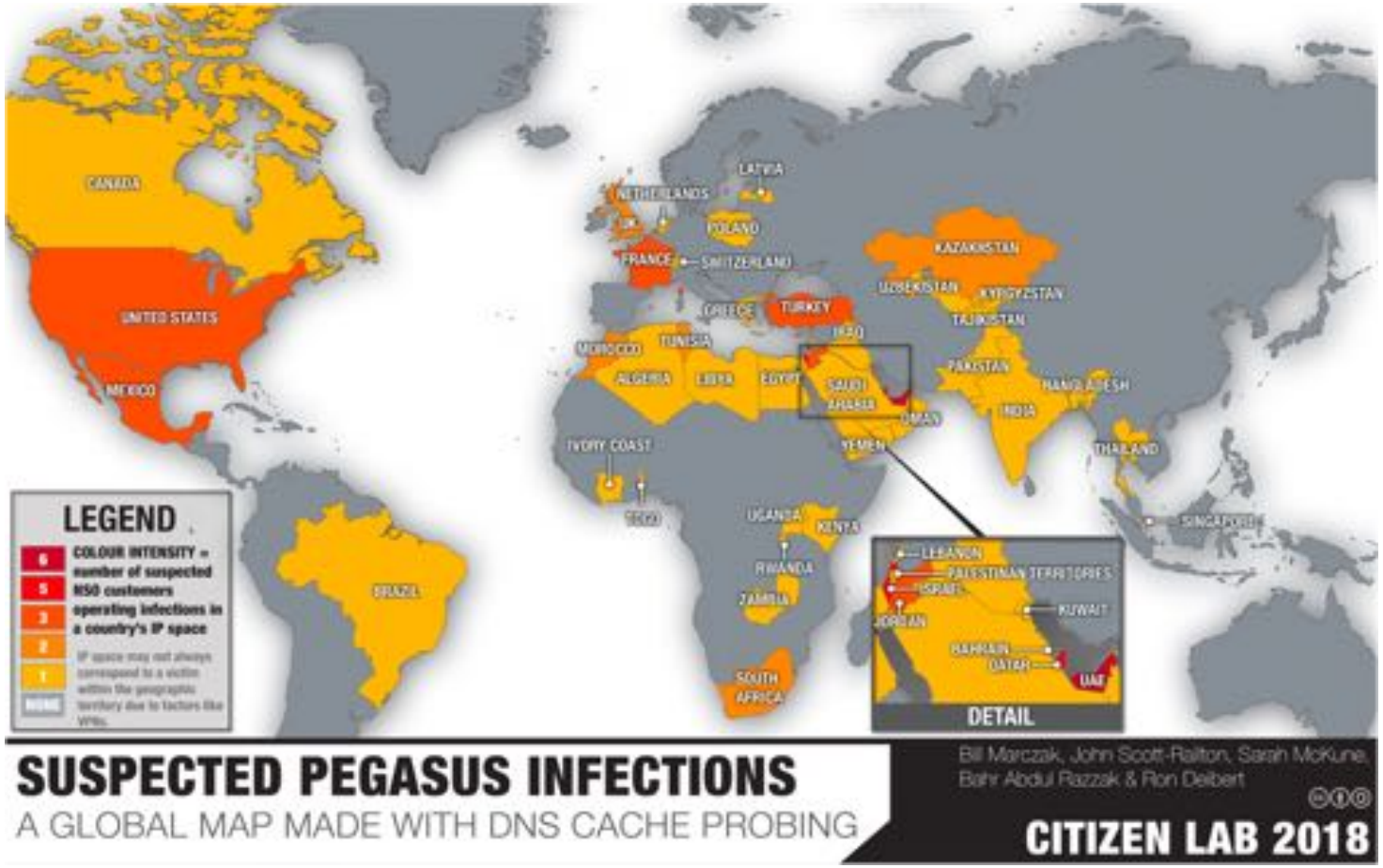

Alex Ionescu
@aionescu
Following
As some of you know, been playing with DirectX lately. A lot of cool ways to bypass EDR/Endpoint tools, especially when it comes 'file-less'/memory injection techniques. The API surface is a pain to learn, but the integration with the NT kernel means lots of fun. Talk for 2019?
6:06 PM - 29 Sep 2018
14 Retweets 72 Likes
5
14
72

2017 was a rough year for SWIFT but!

- SWIFT 7.2!
  - Deadline: November 30, 2018
- Total upgrade of system requirements for SWIFT customers
  - SWIFT Alliance Gateway & SWIFTNet Link moves to 64-bits!
  - Upgrade hardware (x64 only)
    - If older than 2 years old.
  - Upgrade the O.S. (AIX 7.2, RHEL 7.2, Solaris 11.3, Windows 2016)
- Guideline encourages to install the new O.S. with a fresh environment. Inevitable due to the hardware requirements.
  - Prevents persistent attacks to stay on the server side. But… Is it enough?
- No public mention of hardening. SecureBoot? (Fancy Bear's UEFI Rootkits)

IR in Developing Countries?

- Extremely vulnerable to attackers.
- Key targets. This map are only Pegasus infections.



Proactive security

- ARMv8.3 Pointer Authentication
  - New instructions to sign and authenticate pointers
- Capability Hardware Enhanced RISC Instructions (CHERI)
- Intel Threat Detection Technology
  - Advanced Memory Scanner
  - Advanced Platform Telemetry
- O.S. vendors becoming security companies.
  - ATP announced their own EDR...
- SGX/VSM based security
  - Octagon Project.
  - Only a matter of time to see rootkits leveraging that.
- Zero Trust Networks

Matt Suiche @msuiche · 2h

I see more and more runtime solutions for memory scanning/fileless malware (e.g. cloudblogs.microsoft.com/microsoftsecur…, Intel AMS etc.)
Where do you see offline-based memory forensics (for DFIR) in 6 months?

Out of sight but not invisible: Defeating fileless mal…
Removing the need for files is the next progression of attacker techniques. While fileless techniques used to be employed almost exclusively in sophisticated cyber...
cloudblogs.microsoft.com

1 1 4

Shane
@Shane_in_SC
Following

Replying to @msuiche

Still important. Insurance, audit, litigation, and caution all dictate evidence. Alerts are clues but false negatives will hurt you. Forensics produce evidence relating the clues.

10:16 PM - 27 Sep 2018

Matt Suiche @msuiche · 1h

That's the best definition of Forensics I've seen so far. What about Incident Response, is that still considered Forensics?

3

Shane
@Shane_in_SC
Following

Replying to @msuiche

Memory forensics is even more crucial than disk today - many malware are context dependent on the state of their installation (such as user profile) and utilize in memory ONLY configs. Change the state and they false flag another config. Too many in IR don't understand that.

11:04 PM - 27 Sep 2018

The Rise of Cryptocurrency

- TheShadowBrokers has been a pioneer in private coins
  - Zcash (Hybrid private/public ledger)
  - Monero (CryptoNote-based, private ledger)
- Surge in coins
- Poor security of exchanges and smart-contract (see Porosity at DEFCON 25)
- Very hard to track private coins/blockchain transactions
  - Unlike Bitcoin transactions
- Lots of problematics for DFIR.

Thank You!

msuiche@comae.com
@msuiche

References

- April, 2017 – TheShadowBrokers: NSA compromised the SWIFT Network
  - https://blog.comae.io/the-nsa-compromised-swift-network-50ec3000b195
- August, 2017 – TheShadowBrokers: Cyber Fear Game Changers
  - https://blog.comae.io/the-shadow-brokers-cyber-fear-game-changers-d143796f560f
- August 2017 – TheShadowBrokers: WhitePaper
  - https://www.comae.com/reports/us-17-Suiche-TheShadowBrokers-Cyber-Fear-Game-Changers-wp.pdf
- SwitHak TSB's Study
  - https://swithak.github.io/SH20TAATSB18/Study/Summary/
- zerosum0x0 DEFCON Workshop
  - https://github.com/zerosum0x0/defcon-25-workshop
- Piotr Bania on MS09-050
  - https://blog.rapid7.com/2009/10/04/smb2-351-packets-from-the-trampoline/
- Out of sight but not invisible: Defeating fileless malware with behavior monitoring, AMSI, and next-gen AV
  - https://cloudblogs.microsoft.com/microsoftsecure/2018/09/27/out-of-sight-but-not-invisible-defeating-fileless-malware-with-behavior-monitoring-amsi-and-next-gen-av/
- Rethinking logging for critical assets
  - https://blog.comae.io/rethinking-logging-for-critical-assets-685c65423dc0