CYLANCE™ CONSULTING

LESSONS FROM THE WANNACRY / ICS TRENCHES

WHERE ARE WE HEADED, AND HOW DO WE RESTORE TIME TO OUR ADVANTAGE?

Scott Scheferman
Director of Consulting

MISSION

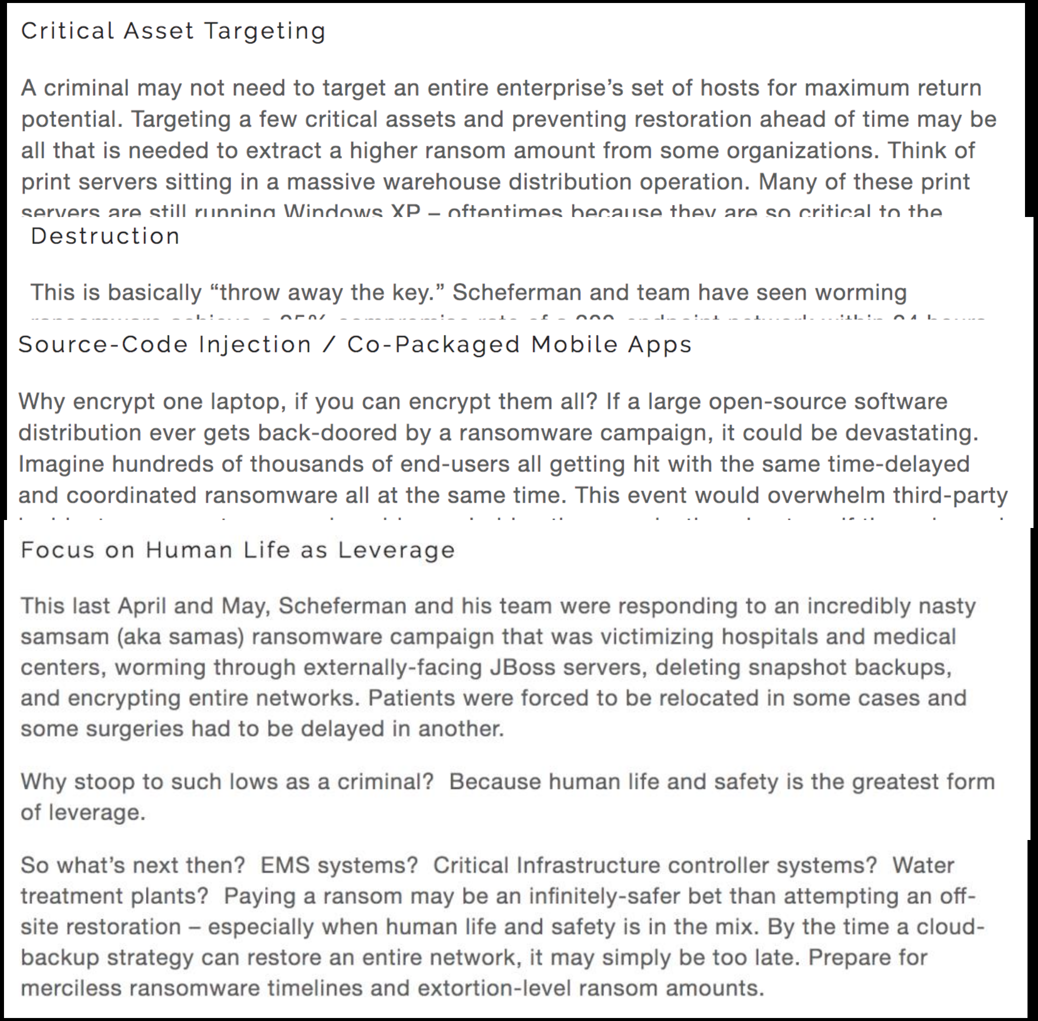
Protect my little warfighter

DoD is FULL of ICS where safety/life, mission availability and operational challenges can often mirror traditional ICS environments in Energy, O&G

That said, I am not an ICS expert

HUMAN PREDICTIONS

- July 2016 article in ITSP



Critical Asset Targeting

A criminal may not need to target an entire enterprise's set of hosts for maximum return potential. Targeting a few critical assets and preventing restoration ahead of time may be all that is needed to extract a higher ransom amount from some organizations. Think of print servers sitting in a massive warehouse distribution operation. Many of these print servers are still running Windows XP – oftentimes because they are so critical to the

Destruction

This is basically "throw away the key." Scheferman and team have seen worming

Source-Code Injection / Co-Packaged Mobile Apps

Why encrypt one laptop, if you can encrypt them all? If a large open-source software distribution ever gets back-doored by a ransomware campaign, it could be devastating. Imagine hundreds of thousands of end-users all getting hit with the same time-delayed and coordinated ransomware all at the same time. This event would overwhelm third-party

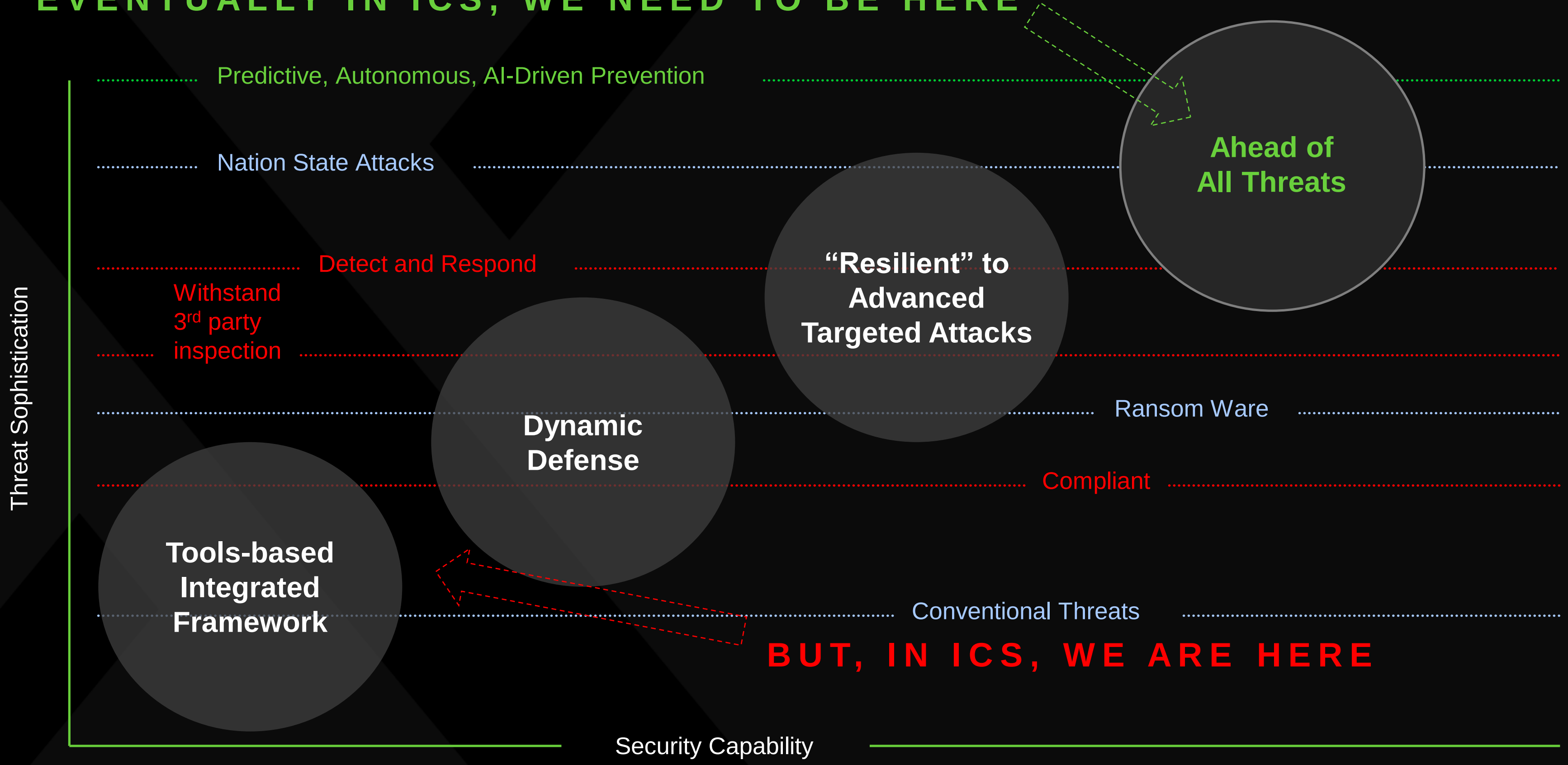
Focus on Human Life as Leverage

This last April and May, Scheferman and his team were responding to an incredibly nasty samsam (aka samas) ransomware campaign that was victimizing hospitals and medical centers, worming through externally-facing JBoss servers, deleting snapshot backups, and encrypting entire networks. Patients were forced to be relocated in some cases and some surgeries had to be delayed in another.

Why stoop to such lows as a criminal? Because human life and safety is the greatest form of leverage.

So what's next then? EMS systems? Critical Infrastructure controller systems? Water treatment plants? Paying a ransom may be an infinitely-safer bet than attempting an off-site restoration – especially when human life and safety is in the mix. By the time a cloud-backup strategy can restore an entire network, it may simply be too late. Prepare for merciless ransomware timelines and extortion-level ransom amounts.

EVENTUALLY IN ICS, WE NEED TO BE HERE



Predictive, Autonomous, AI-Driven Prevention

Nation State Attacks

Detect and Respond

Withstand
3rd party
inspection

Ransom Ware

Compliant

Conventional Threats

Ahead of
All Threats

“Resilient” to
Advanced
Targeted Attacks

Dynamic
Defense

Tools-based
Integrated
Framework

BUT, IN ICS, WE ARE HERE

“It is a renaissance, it is a golden age… we are now solving problems with ML and AI that were in the realm of science fiction for the last several decades…ML and AI is a horizontal-enabling layer, it will empower and improve every business, every government organization, philanthropy, basically *there is no institution in the world that cannot be improved with ML”*

Jeff Bezos, CEO of Amazon

ALPHA (PREDICTIVE AI)

During simulated aerial engagements with ALPHA, Lee could not score a single kill and was repeatedly shot out of the air.

ALPHA processes sensor data and plans combat moves … over 250 times faster than the eye can blink — reaction times far beyond human abilities…

And it runs on a $500 laptop…

“It seemed to be aware of my intentions and reacting instantly to my changes in flight and my missile deployment. It knew how to defeat the shot I was taking.”

RETIRED AIR FORCE
COLONEL GENE LEE

EA-18G GROWLER AND *PREDICTIVE* "COGNITIVE ELECTRONIC WARFARE"

"[…] we respond and **react faster than human timescales**, […] scouring the spectrum in real time and applying […] artificial intelligence. [Then we] build onboard systems that can learn what the adversary is doing in the electromagnetic spectrum**, start making predictions about what they're going to do next**, and then adapt the onboard jammer **to be where the adversary's going before they get there."**

DARPA DIRECTOR ARATI PRABHAKA

NETFLIX PREDICTIVE AI

NETFLIX

Netflix's predictive AI is so effective that now you don't even have to use a 5 star rating system for it to know what you'll want to watch for years to come…all based on a predictive self-learning A.I. that knows your movie/TV tastes in ways you'll likely never even comprehend yourself.

Netflix found that customers, on average, give up 90 seconds after searching for a movie. By improving search results, Netflix projects that they have avoided canceled subscriptions enough to prevent $1B of losses every year. ($2.7m/day!)

BETTERMENT RETIREMENT INVESTING
AKA: ROBO-ADVISING

Jon Stein, CEO of Betterment, a fast-growing A.I. “robo-advisor” for personal finance and investment decision-making, said “When Betterment started, there was a lot of fear that the human role [of investment advisor] would disappear. But that did not happen. Each person instead can now serve more customers better.” Longtime New York venture capitalist Alan Patricof chimed in to say “We’re going into a phase where we’re teaching ourselves to get better and better” through the use of computing.

IF TIME WAS A SPEAR…

KNOWN THREATS

UNKNOWN THREATS

AHEAD OF *ALL* THREATS

Legacy Antivirus
NG Firewalls
Web Proxies
IDS/IPS
All Signature/Heuristic-Based Tech

Detonation Chambers, Call-back Detection, Anomalytics, Cyber Threat Intelligence

PREDICTIVE AI

TEMPORAL ADVANTAGE

To put it simply: threat actors have had a *temporal advantage* over us. We have been playing catch-up for decades, especially in ICS/OT

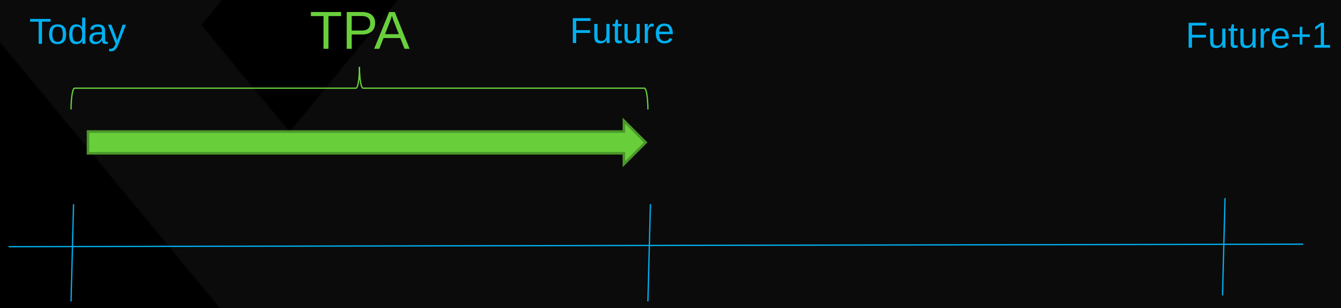
INTRODUCING THE TEMPORAL PREDICTIVE ADVANTAGE

What is it?

The Ability to Predict and Be where the Enemy is Going to be Before they Get There

“The number of days by which Predictive AI is able to *successfully predict and prevent* the execution of threats, *prior to the date of the first industry report* on that threat campaign ....and do so *without need for the cloud.”*

TEMPORAL PREDICTION ADVANTAGE



Today

TPA

Future

Future+1

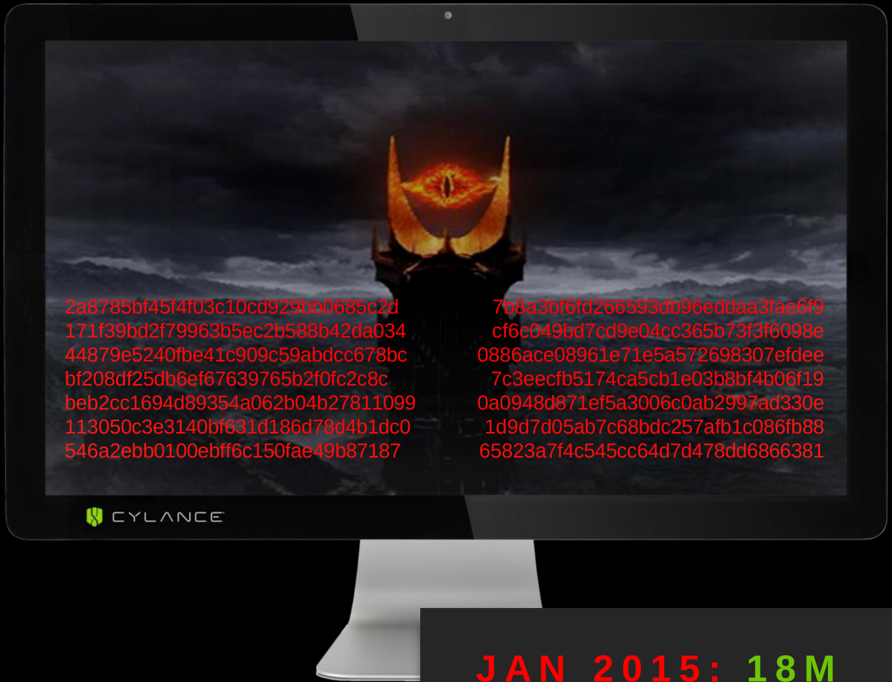
Predictive Win
Preventing
Execution of
Unknown Threats,
Prior to Any Human
Knowable Threat
Intelligence,
Signatures, or even
a “Patient Zero”

Day Zero
Report
Comes
out…aka
“Patient Zero”
Like 5/12/17
for WannaCry
Ransomware

Signatures /
Heuristics /
Intel Feeds /
IOCs /
Reputation /
Attribution
Become
Operationalized
(The ‘rest of
industry’ has
semi-protection)

SAURON/ STRIDER/ REMSEC

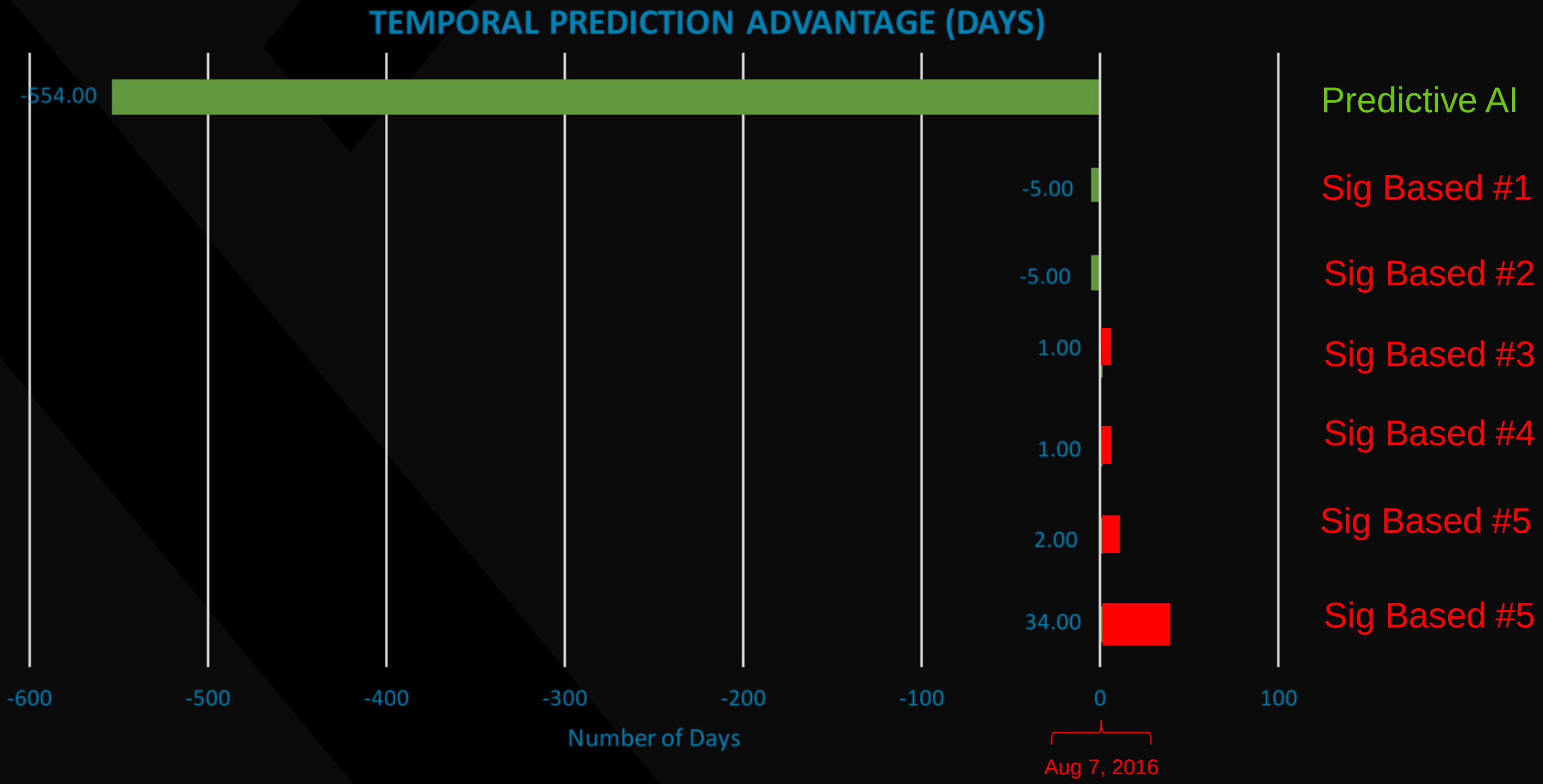
- Espionage Backdoor dating back to 2011. Undetected until
- Human Discovered August 2016
- Uses blobs (Binary Large Objects), LUA, and memory resident code over the network to evade detection



```
2a8785bf45f4f03c10cd929bb0685c2d      7b8a3bf6fd266593db96eddaa3fae6f9
171f39bd2f79963b5ec2b588b42da034      cf6c049bd7cd9e04cc365b73f3f6098e
44879e5240fbe41c909c59abdcc678bc      0886ace08961e71e5a572698307efdee
bf208df25db6ef67639765b2f0fc2c8c      7c3eecfb5174ca5cb1e03b8bf4b06f19
beb2cc1694d89354a062b04b27811099      0a0948d871ef5a3006c0ab2997ad330e
113050c3e3140bf631d186d78d4b1dc0      1d9d7d05ab7c68bdc257afb1c086fb88
546a2ebb0100ebff6c150fae49b87187      65823a7f4c545cc64d7d478dd6866381
```

JAN 2015: 18M
Prior to human discovery

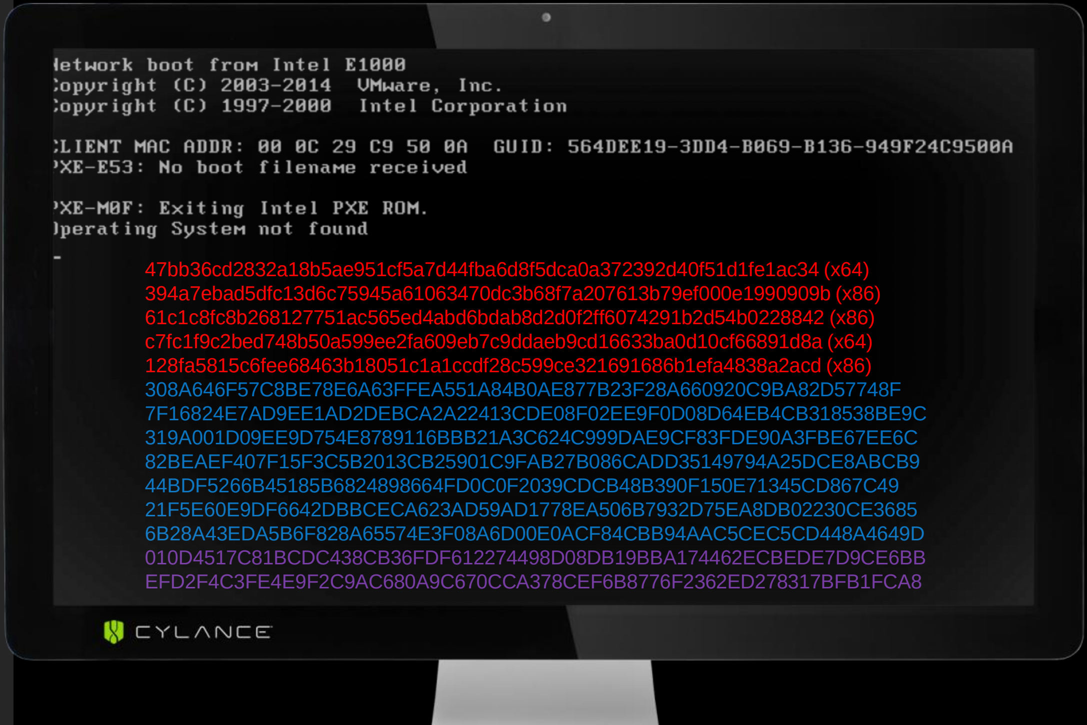
REMSEC: 2a8785bf45f4f03c10cd929bb0685c2d



CYLANCE CONSULTING

SHAMOON 2 / WAVE 2

- Energy / S.A. Focused, destructive, leverages hard-coded user account/passwords to target related VDI systems, and destroys MBR
- Human Discovered by PAN Unit42 on
  Nov 30 2016 Shamoon 2
  Jan 9 2017   Shamoon 2, 2nd Wave
- Human Discovered by Symantec on
  Jan 23 2017 GreenBurg (PW stealer)



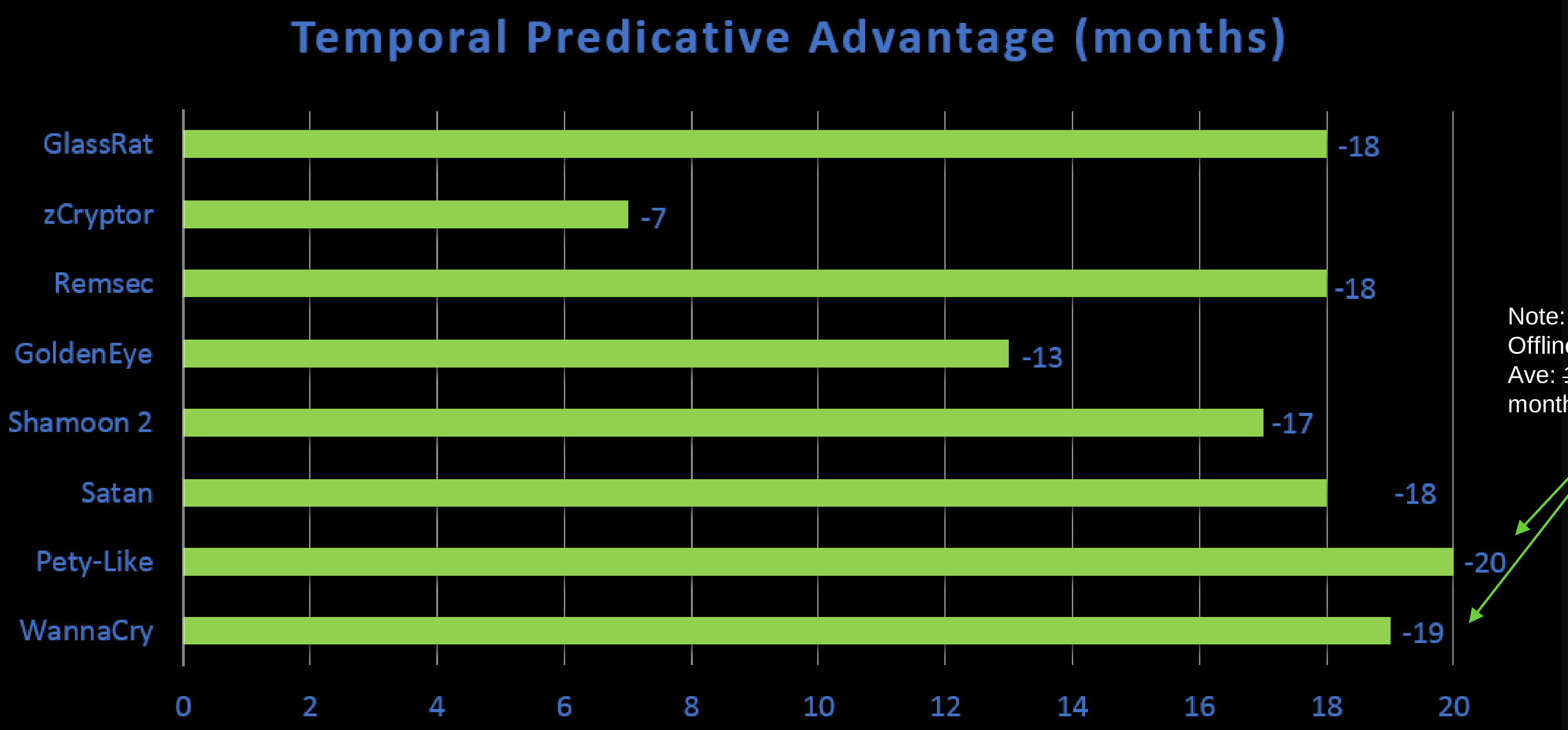
```
letwork boot from Intel E1000
Copyright (C) 2003-2014  VMware, Inc.
Copyright (C) 1997-2000  Intel Corporation

CLIENT MAC ADDR: 00 0C 29 C9 50 0A  GUID: 564DEE19-3DD4-B069-B136-949F24C9500A
PXE-E53: No boot filename received

PXE-M0F: Exiting Intel PXE ROM.
Operating System not found
_
```

```
47bb36cd2832a18b5ae951cf5a7d44fba6d8f5dca0a372392d40f51d1fe1ac34 (x64)
394a7ebad5dfc13d6c75945a61063470dc3b68f7a207613b79ef000e1990909b (x86)
61c1c8fc8b268127751ac565ed4abd6bdab8d2d0f2ff6074291b2d54b0228842 (x86)
c7fc1f9c2bed748b50a599ee2fa609eb7c9ddaeb9cd16633ba0d10cf66891d8a (x64)
128fa5815c6fee68463b18051c1a1ccdf28c599ce321691686b1efa4838a2acd (x86)
308A646F57C8BE78E6A63FFEA551A84B0AE877B23F28A660920C9BA82D57748F
7F16824E7AD9EE1AD2DEBCA2A22413CDE08F02EE9F0D08D64EB4CB318538BE9C
319A001D09EE9D754E8789116BBB21A3C624C999DAE9CF83FDE90A3FBE67EE6C
82BEAEF407F15F3C5B2013CB25901C9FAB27B086CADD35149794A25DCE8ABCB9
44BDF5266B45185B6824898664FD0C0F2039CDCB48B390F150E71345CD867C49
21F5E60E9DF6642DBBCECA623AD59AD1778EA506B7932D75EA8DB02230CE3685
6B28A43EDA5B6F828A65574E3F08A6D00E0ACF84CBB94AAC5CEC5CD448A4649D
010D4517C81BCDC438CB36FDF612274498D08DB19BBA174462ECBEDE7D9CE6BB
EFD2F4C3FE4E9F2C9AC680A9C670CCA378CEF6B8776F2362ED278317BFB1FCA8
```

Shamoon 2: 483D
GreenBurg: 517D
Shamoon 2/W2: 523D
Prior to human discovery



Note:
Offline Mode
Ave: ~~15.0~~ 16.5
months

CYLANCE
CONSULTING

So, why not leverage Predictive AI when we are conducting Compromise Assessments & Incident Response?

And for Beyond Just Malware…

QUAKBOT IN OR NEAR ICS…. ?

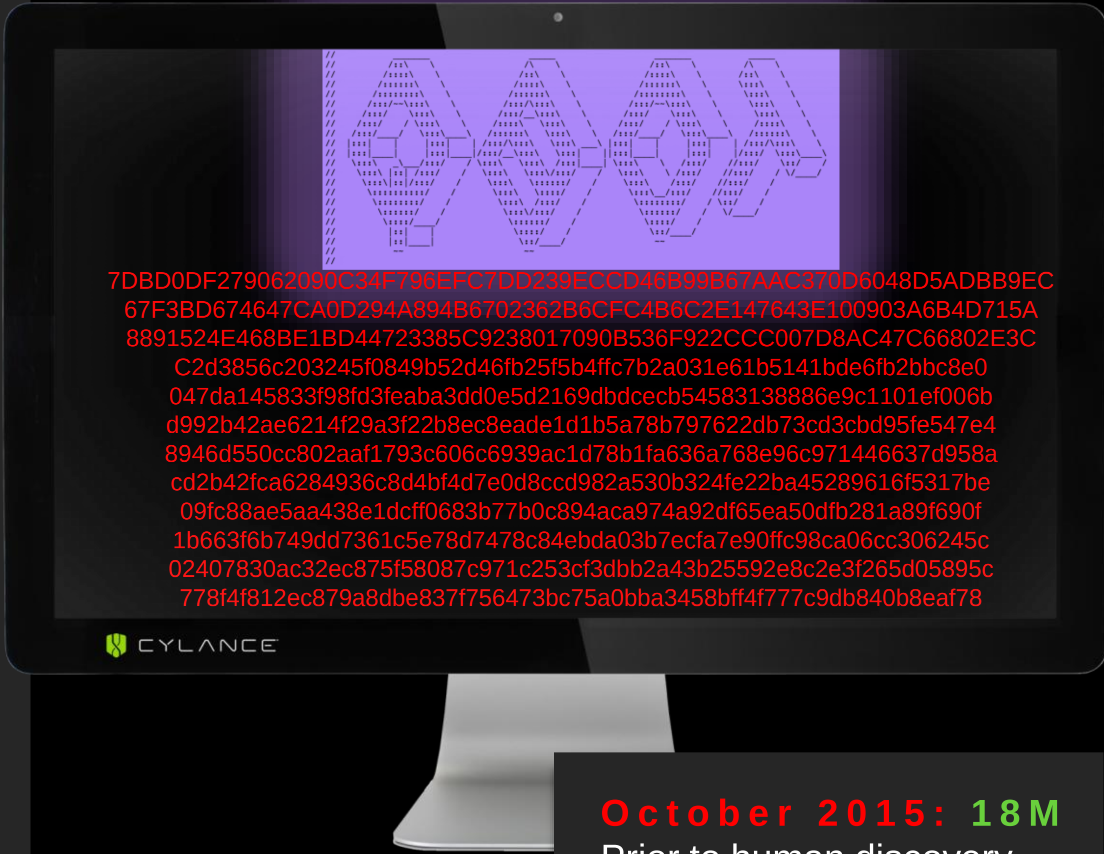
- QuakBot / Qbot is making a massive come-back in 2017
- 13 active IR’s going on right now
- Low detection rates (<25%), highly evasive, polymorphic
- Proactively mining this campaign given our AI predicted this +17 months ago (via fuzzy hashing to work backwards from the AI)
- Reworked to target 64-bit browsers = no small feat / investment
- Multi-threaded = likely a new author. Cleaner code, efficiency gains
- RNG code un-changed
- 20% of code is Persistence Mechanisms that bypass: Microsoft, McAfee, AVG, Kaspersky, NOD32, BitDefender, Avast, TrendMicro. Knocks Windows Defender completely offline
- Int’l Character Support and affecting output at several Int’l ICS clients
- Fully contained via AI during IR’s

NOW THINK ABOUT YOUR OWN ICS – THE IT/OT CREDENTIALS CONNECTION

- No stones are left unturned!
  - It can easily lock out thousands of accounts in quick succession
  - Rapid automated logon attempts, some launched using accounts that do not exist
  - Deploys malicious executables to network shares & registers them as a service
  - No accounts are off limits: backup, sql, DA, application PWs
  - MITM Browser for code injection and password theft via fake logins
  - Keystroke logger
  - HTTPS auth data, digi certs, cached creds, cookies, FTP/POP3, tokens
  - Recon! IP/DNS/hostname, domain, user privs, software list, protected storage creds (all things to point to your ICS!)

QBOT / QAKBOT 2017

- Largely rewritten from ground up: 64-bit, multi-threaded, multi-national
- Evades/Persists vs. Microsoft, McAfee, AVG, Kaspersky, NOD 32, BitDefender, Avast, and TrendMicro Legacy A/V
- Rapidly evolving, uses DGA's, locks out entire enterprises, steals creds
- Vertical-agnostic this time (not just FIN)
- Human-Discovered: April 2017

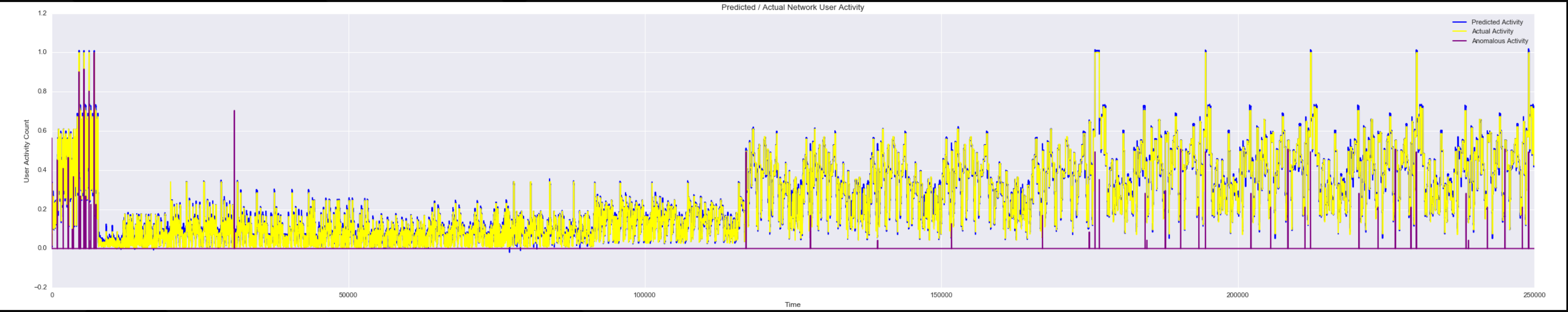


```
7DBD0DF279062090C34F796EFC7DD239ECCD46B99B67AAC370D6048D5ADBB9EC
67F3BD674647CA0D294A894B6702362B6CFC4B6C2E147643E100903A6B4D715A
8891524E468BE1BD44723385C9238017090B536F922CCC007D8AC47C66802E3C
C2d3856c203245f0849b52d46fb25f5b4ffc7b2a031e61b5141bde6fb2bbc8e0
047da145833f98fd3feaba3dd0e5d2169dbdcecb54583138886e9c1101ef006b
d992b42ae6214f29a3f22b8ec8eade1d1b5a78b797622db73cd3cbd95fe547e4
8946d550cc802aaf1793c606c6939ac1d78b1fa636a768e96c971446637d958a
cd2b42fca6284936c8d4bf4d7e0d8ccd982a530b324fe22ba45289616f5317be
09fc88ae5aa438e1dcff0683b77b0c894aca974a92df65ea50dfb281a89f690f
1b663f6b749dd7361c5e78d7478c84ebda03b7ecfa7e90ffc98ca06cc306245c
02407830ac32ec875f58087c971c253cf3dbb2a43b25592e8c2e3f265d05895c
778f4f812ec879a8dbe837f756473bc75a0bba3458bff4f777c9db840b8eaf78
```

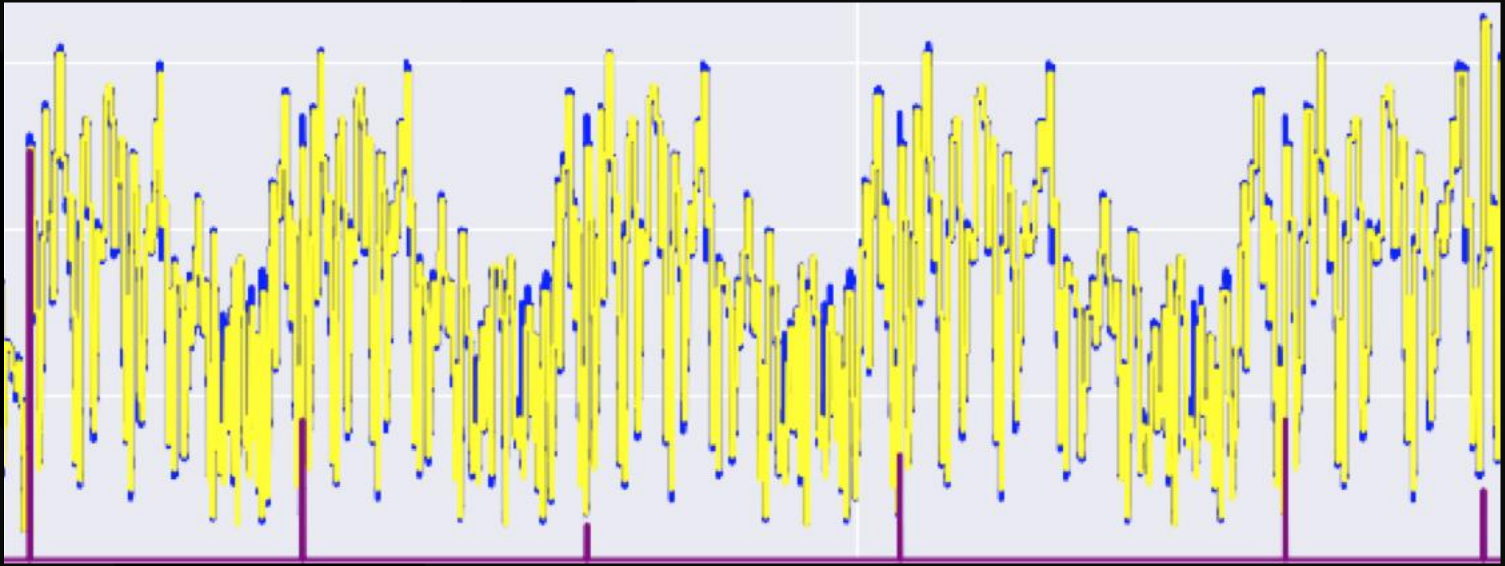
October 2015: 18M
Prior to human discovery

WHILE ON THE SUBJECT OF CREDENTIALS… HOW DO YOU KNOW WHEN YOUR ACCOUNTS ARE COMPROMISED?

The User Account Activity AI kind of looks like this for a 10,000+ device network



The Irony of applying AI to *more* data, where *bigger is *easier**



| = Actual | = Predicted | = Anomaly (The higher the peak the more anomalous the event) |

The Math Goes a Little Something like This….

- Looks at over 100 discreet event types and normalizes event data
- An auto encoder neural network preprocesses clusters into separated groups
- Feeds into a recurrent neural network model using Long Short-Term Memory (LTSM) hidden layers:
  - Used to model out regular user / network activity and make predictions
  - Calculates the difference of the model's predictions to the actual activity and then calculates standard deviation
  - Finds outlier time slices to point back to compromised accounts
- Ability to monitor either individual users or the entire network of users
- Takes into account scheduled events that would otherwise trigger an anomaly (FPs)
  - Uses memory cells to record and consider events like mass-logons during device inventory scans
- Constantly improves over time, yielding higher confidence and faster results

Let’s take a quick look at WANNACRY

Who Could Have Predicted *WannaCry?*

WANNACRY WORM PREDICTION

Who could have predicted that a worm (which we haven’t seen the likes of in nearly a decade) would have taken out hospital systems, two airlines, railway systems, 2 automobile manufactures, shipping companies, power companies, police departments, ATMs, and even laundry mat machines around the world, over 230,000 machines, in one weekend?

HOW DID WANNACRY ORIGINATE

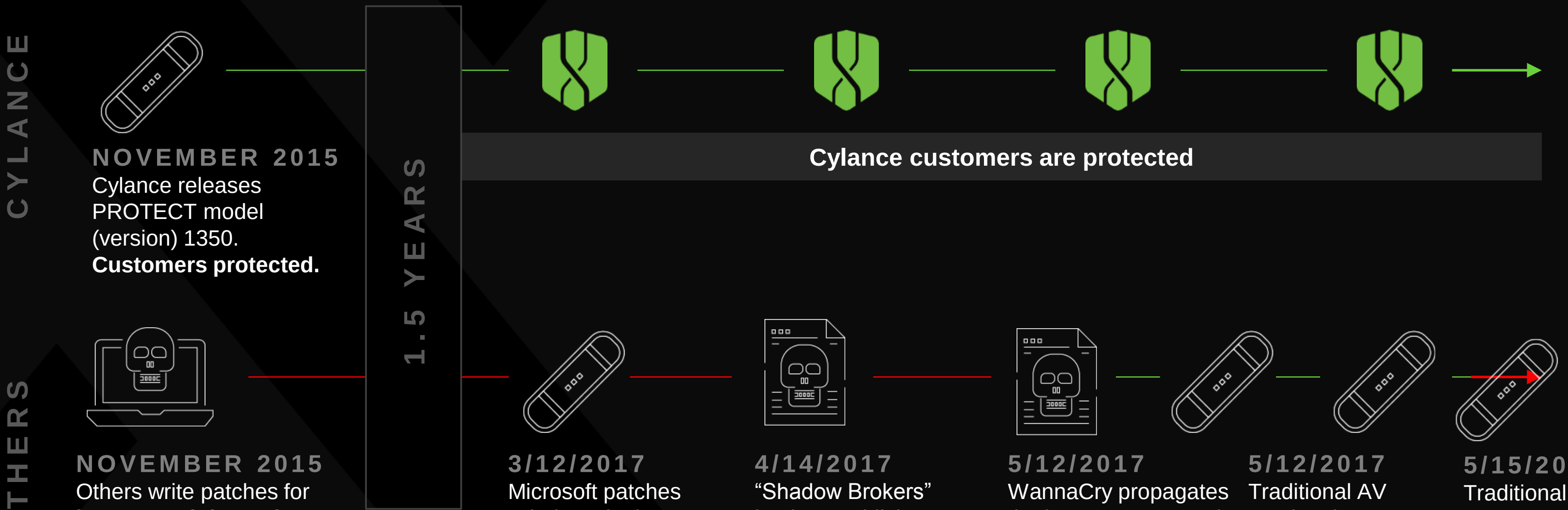
- NSA discovered the ‘EternalBlue’ exploit
- Disclosed by Shadow Brokers dump in April 2017
- Microsoft issues patch in April 2017 as critical security bulletin MS17-010
- Flaw was so critical that even Windows XP patched
- First sample on Virus Total March 20 2017
- Major outbreak started in EMEA Friday May 12 2017 and continues

CYLANCE WANNACRY TEMPORAL PREDICTIVE ADVANTAGE

What happens when the hash changes? Or the hack method changes?

PROTECTED

VULNERABLE



Cylance customers are protected

NOVEMBER 2015
Cylance releases PROTECT model (version) 1350.
Customers protected.

NOVEMBER 2015
Others write patches for **known exploits at the time, but not for EB.** Microsoft Windows is vulnerable is vulnerable to EB.

3/12/2017
Microsoft patches Windows for known vulnerabilities. **Not everyone updates.**

4/14/2017
“Shadow Brokers” hackers publish trove of NSA attack method documents

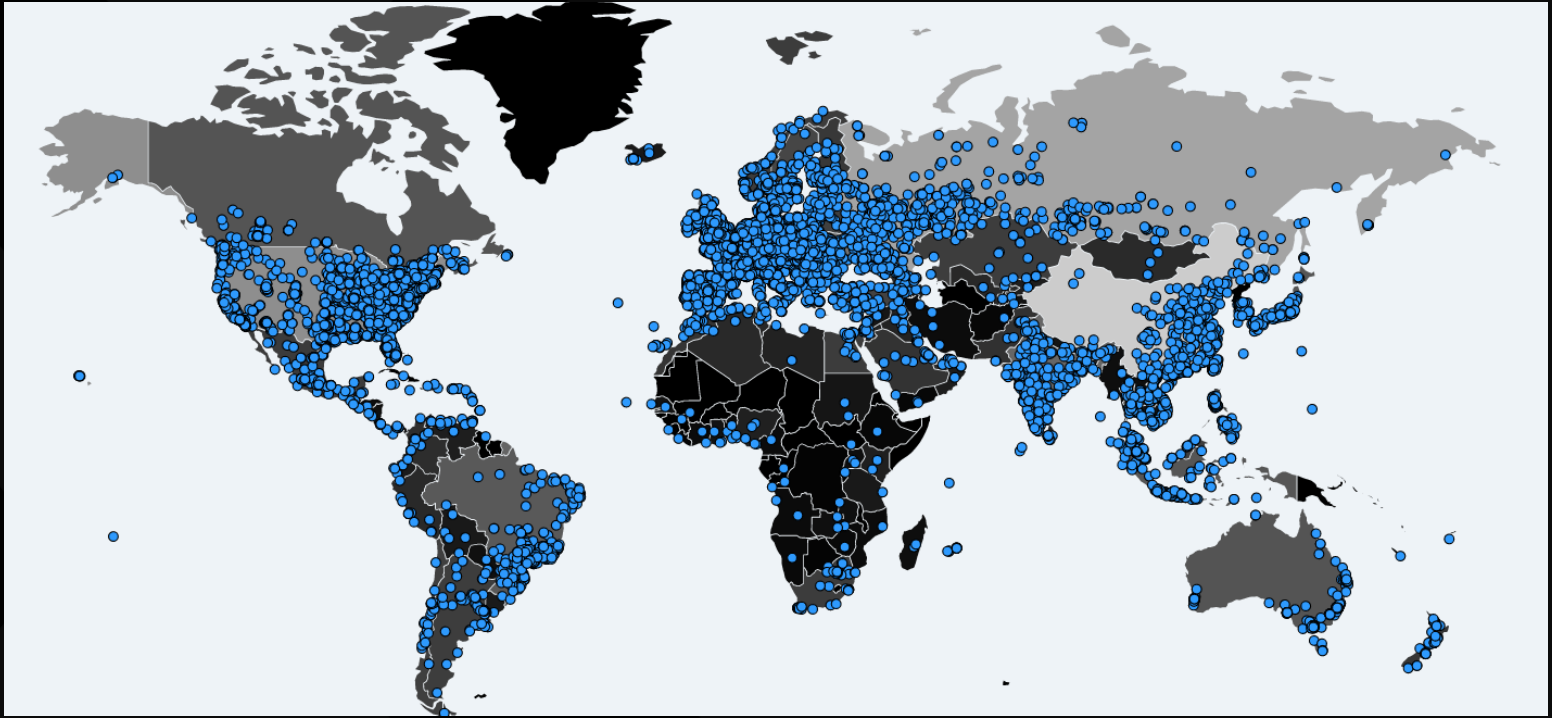
5/12/2017
WannaCry propagates the internet. Impacted:

- Healthcare
- Government
- Logistics
- Transportation
- Manufacturing
- Financial Services

5/12/2017
Traditional AV vendors issue signatures, patches, and help articles.

5/15/2017
Traditional AV vendors issue emergency DAT files for WannaCry variants

300,000 INFECTIONS ACROSS 150 COUNTRIES



***Source**: http://news.thewindowsclub.com/wannacry-ransomware-attack-spreads-89665/*

SOME OF WHAT WE LEARNED ABOUT THE BATTLE

*Devices that can’t be patched or upgraded still need a contingency plan and a place in the DRP

*In some plant environments, SMB v1 is critical to plant operations....you can’t just ‘block it’

*If you do try to disable or block SMB, you can affect your ability to manage and inventory those devices via traditional IT solutions

*You don’t have enough bandwidth in your plant to handle an SMB worm storm... No, really.

*You don’t actually have a full inventory of devices, VDI environments, and many are not label or accounted for. The basics MATTER when you are on your knees. ALL of them.

*It may only take a squad to run a production plant…but it takes an ARMY to turn it back around

Your Vendor SLA’s are part of the reason why

*Your workforce’s ability to expertly restore a diverse array of devices all at once is effectively zero

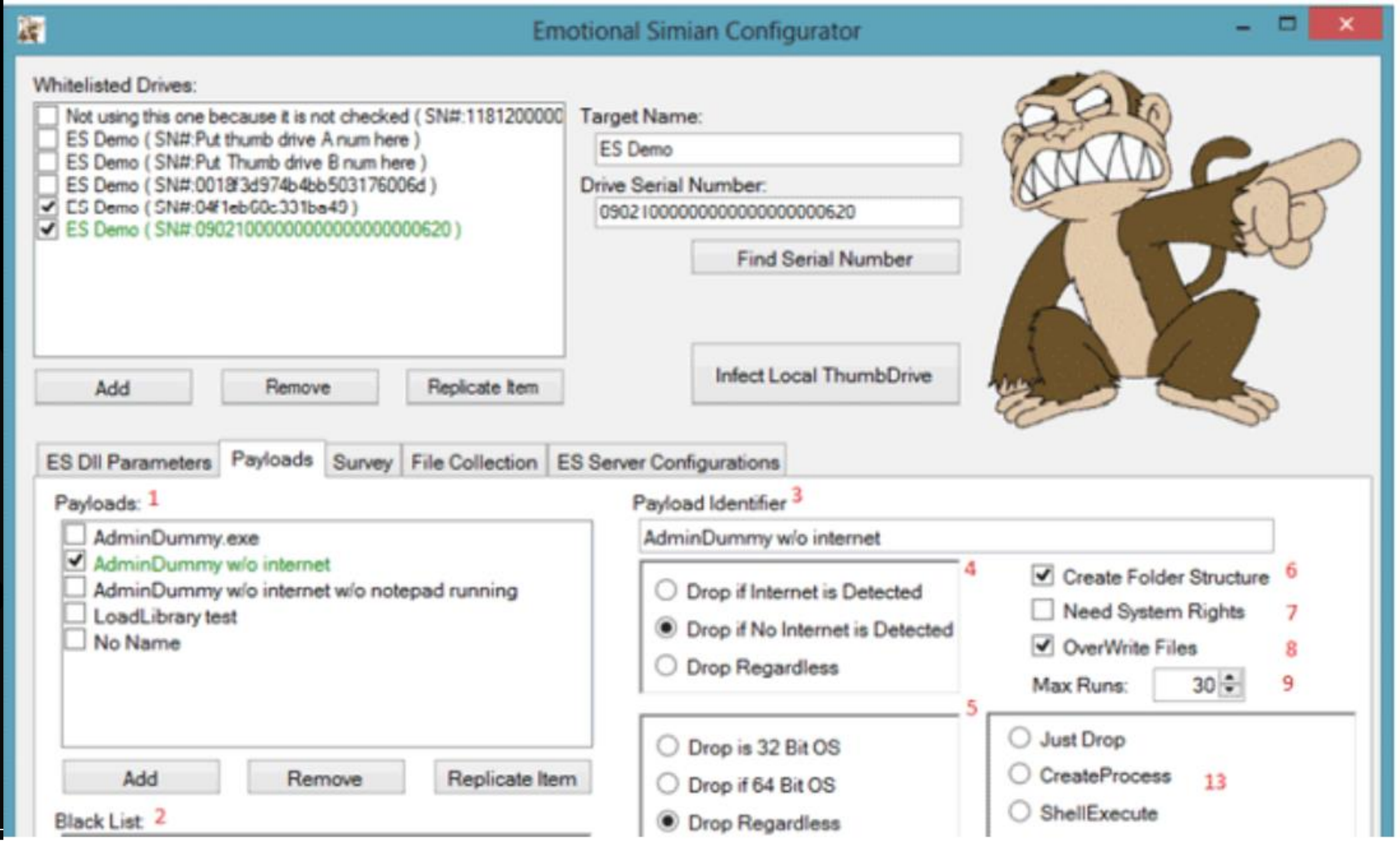
*You won’t have time to worry about attribution, motive, or RCA... Those are luxuries in the face of a worm like Eternal Blue/Double Pulsar

*You have lost all security-control of your environment, there is no going back to ‘business as usual’. Double Pulsar can be used to steal credentials and execute any file on disk, pass commands, etc. It is a *quintessential* OS exploit. Your enterprise becomes swiss cheese for any follow-on attacks, or malicious insiders.

*Be prepared to dev your way out of the rabbit hole, be flexible, and make quick, risk-based decisions. This is true triage, and risk of re-infection and bandwidth storms is high.

*What you think is a ransomware attack may not be...or it may. Proceed under ALL potentialities, don’t pick just one. Corrupted payloads? Creds? Lack of RCA/foothold? Resistant staff?

WHAT IS TO COME?



Emotional Simian Configurator

Whitelisted Drives:

- □ Not using this one because it is not checked (SN#:1181200000
- □ ES Demo (SN#:Put thumb drive A num here)
- □ ES Demo (SN#:Put Thumb drive B num here)
- □ ES Demo (SN#:0018f3d974b4bb503176006d)
- ☑ ES Demo (SN#:04f1eb00c331ba49)
- ☑ ES Demo (SN#:09021000000000000000000620)

Target Name: ES Demo

Drive Serial Number: 0902100000000000000000620

Payloads: 1

- □ AdminDummy.exe
- ☑ AdminDummy w/o internet
- □ AdminDummy w/o internet w/o notepad running
- □ LoadLibrary test
- □ No Name

Black List: 2

Payload Identifier 3: AdminDummy w/o internet

4
- ○ Drop if Internet is Detected
- ● Drop if No Internet is Detected
- ○ Drop Regardless

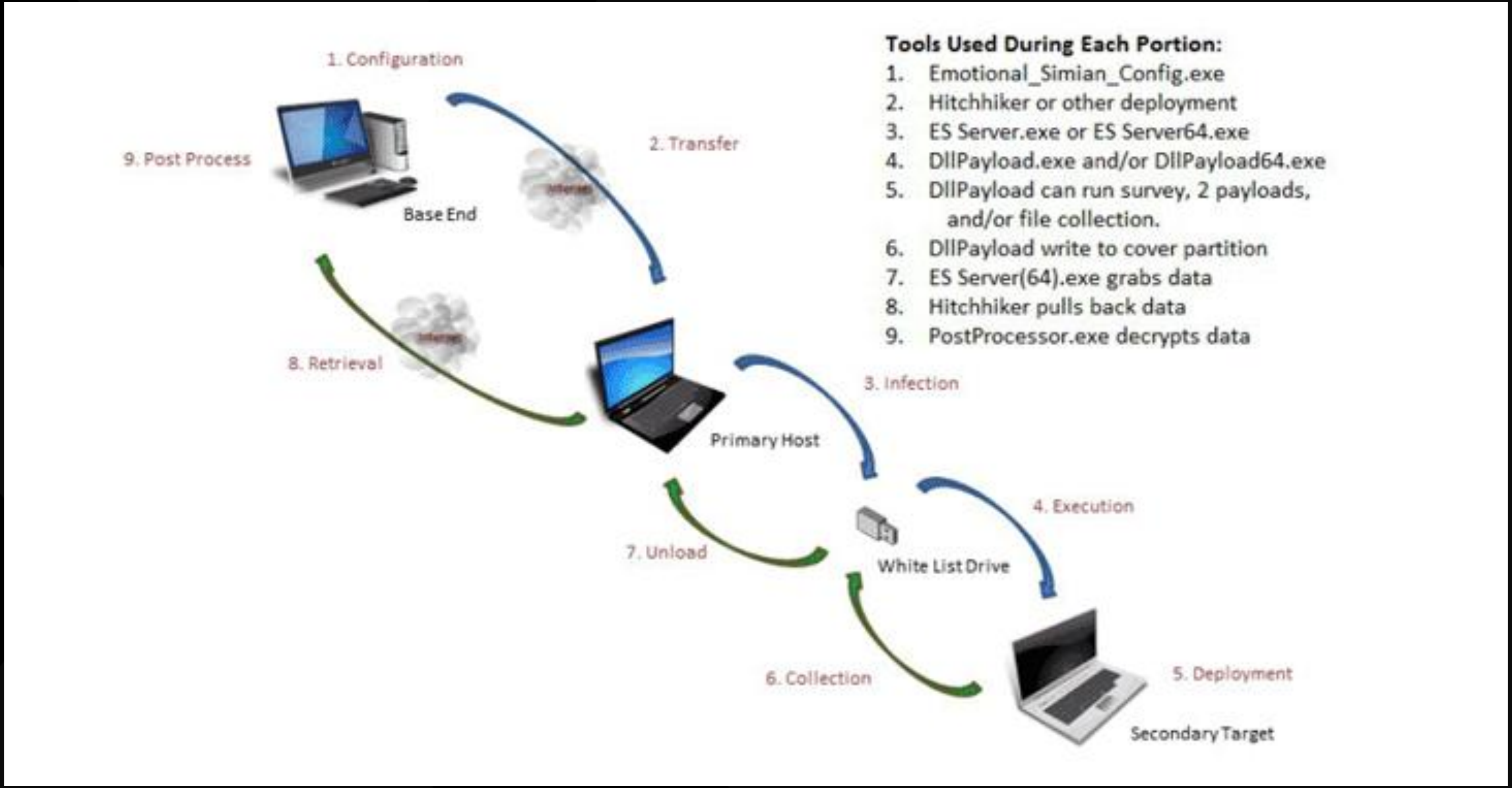
5
- ○ Drop is 32 Bit OS
- ○ Drop if 64 Bit OS
- ● Drop Regardless

- ☑ Create Folder Structure 6
- □ Need System Rights 7
- ☑ OverWrite Files 8

Max Runs: 30 9

13
- ○ Just Drop
- ○ CreateProcess
- ○ ShellExecute

BRUTAL KANGAROO – USB DRIVE EXFIL NETWORK



Tools Used During Each Portion:

1. Emotional_Simian_Config.exe
2. Hitchhiker or other deployment
3. ES Server.exe or ES Server64.exe
4. DllPayload.exe and/or DllPayload64.exe
5. DllPayload can run survey, 2 payloads, and/or file collection.
6. DllPayload write to cover partition
7. ES Server(64).exe grabs data
8. Hitchhiker pulls back data
9. PostProcessor.exe decrypts data

CRASH OVERRIDE – PAVING THE WAY FOR THE PERFECT STORM

- In 2015 the group that attacked Ukraine Power Plants, once maintaining a foothold, were able to manually send commands to breakers.
- In 2017, however, this portion was *automated*, and allowed the malware to continuously send reset commands to breakers
- Worse, this is a modular, regional-agnostic piece of malware that can just as easily target USA.

What happens when this is combined with the concept of ransom leverage? Who cares about encryption, when you can just as easily automate shutting off power?

A NASTY COMBINATION

Eternal Blue/DP meets Qakbot meets Crash Override

Creds (all types for all systems via Qbot)
Lockouts (via Qbots persistent BF’ing)
Air-Gap Jumping (via Brutal Kangaroo, Eternal Blue on Jump Boxes)
Bandwidth Chocking (via EB/DP)
Ransom Leverage (via Crash Override, or a proper crypto function)
ICS/Production/Mission-Critical Impacts (via bandwidth, jumping, creds)

RECOMMENDATION – PATCH OFTEN AND EARLY

?

How are patches and updates handled on your critical control system assets?

Select the most applicable method.

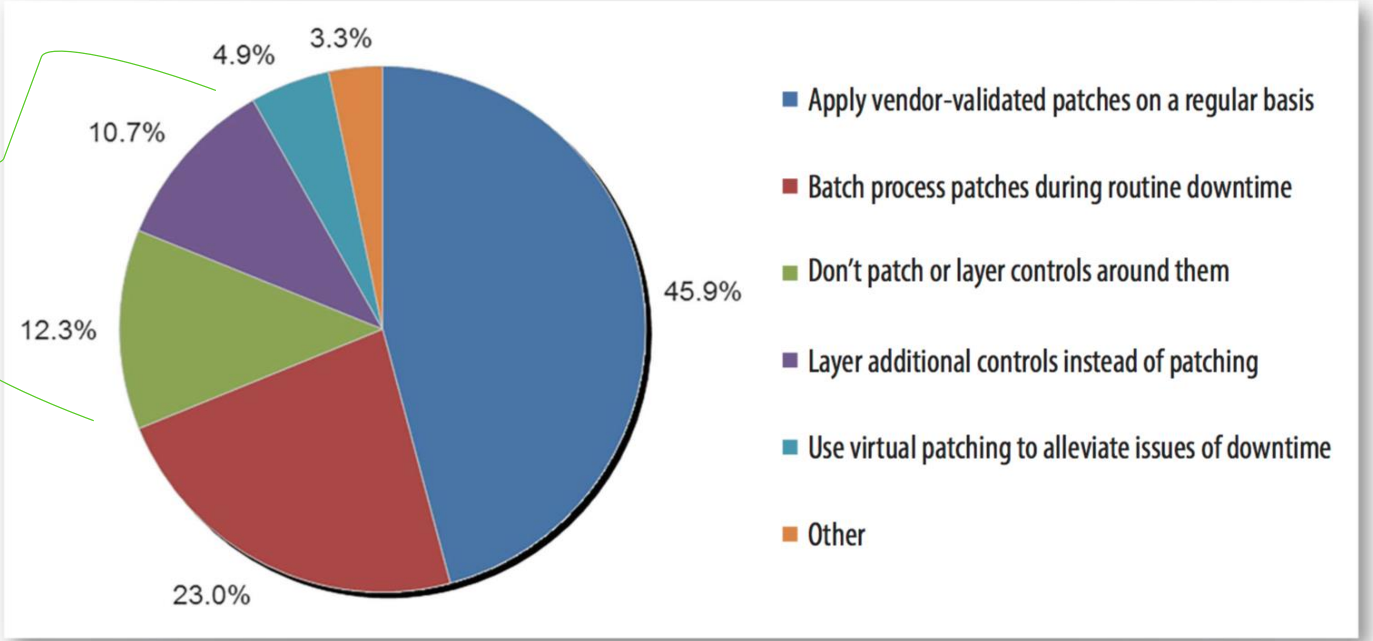


Figure 13. Patching Practices

Ref: https://www.sans.org/reading-room/whitepapers/analyst/securing-industrial-control-systems-2017-37860

RECOMMENDATION – CROSS TRAIN TO CONVERGE

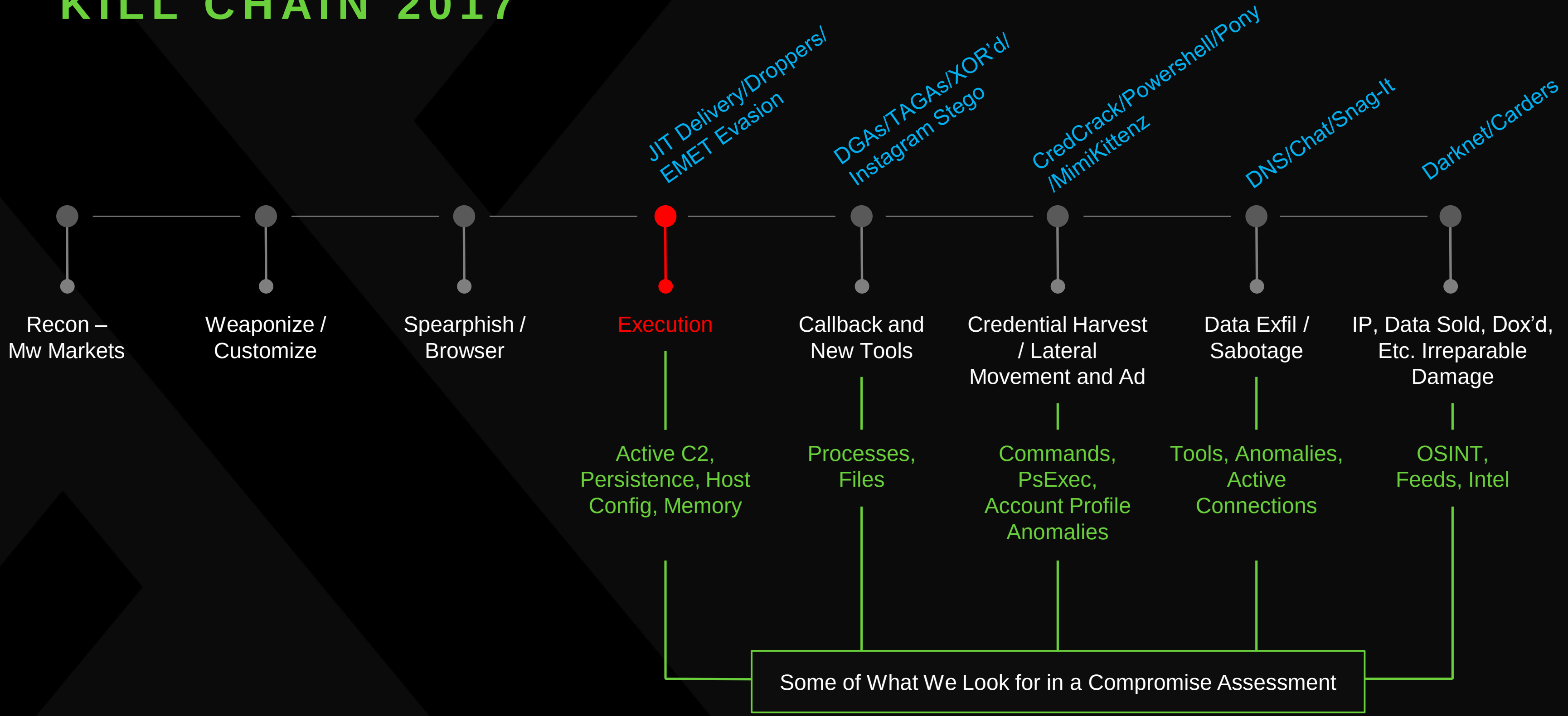
- IT sec person spend 6-months with OT – learn, and then bring back insight to the rest of IT team, and report to the OT management directly during this time
- When teaching OT personnel about spear-phishing and cyber security awareness, tie into the Safety and Awareness training curriculum / culture already in place
- Make Cyber and Safety synonymous

Ref: https://www.sans.org/reading-room/whitepapers/analyst/securing-industrial-control-systems-2017-37860

RECOMMENDATION – WHERE ABLE, LEVERAGE ML/AI

Let’s take a look at the cyber-kill chain to understand why….

KILL CHAIN 2017



Recon – Mw Markets

Weaponize / Customize

Spearphish / Browser

Execution

JIT Delivery/Droppers/ EMET Evasion

Active C2, Persistence, Host Config, Memory

Callback and New Tools

DGAs/TAGAs/XOR'd/ Instagram Stego

Processes, Files

Credential Harvest / Lateral Movement and Ad

CredCrack/Powershell/Pony /MimiKittenz

Commands, PsExec, Account Profile Anomalies

Data Exfil / Sabotage

DNS/Chat/Snag-It

Tools, Anomalies, Active Connections

IP, Data Sold, Dox'd, Etc. Irreparable Damage

Darknet/Carders

OSINT, Feeds, Intel

Some of What We Look for in a Compromise Assessment

AT THE SPEED OF COMPUTING

CYLANCE CONSULTING

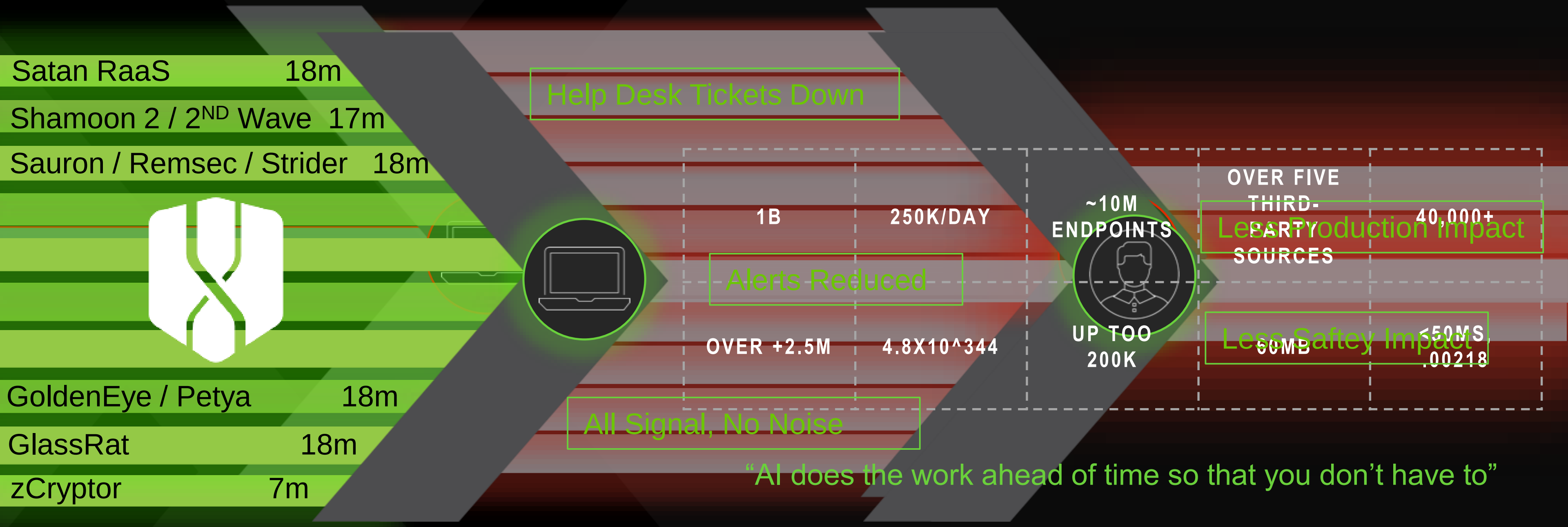
KILL CHAIN – *PREDICTIVE* PREVENTION

KILL CHAIN – LEGACY SIGNATURE-BASED

WORK AND RISK LEVEL

WORK AND RISK LEVEL

Satan RaaS	18m
Shamoon 2 / 2ND Wave	17m
Sauron / Remsec / Strider	18m
GoldenEye / Petya	18m
GlassRat	18m
zCryptor	7m



"AI does the work ahead of time so that you don't have to"

Malware Economy

Signature/Behavior Based Legacy A/V, Low Efficacy

Cylance Predictive AI at 99%

C2

C2

Lateral Movement, Whitelisted Tools, Changing TTPs

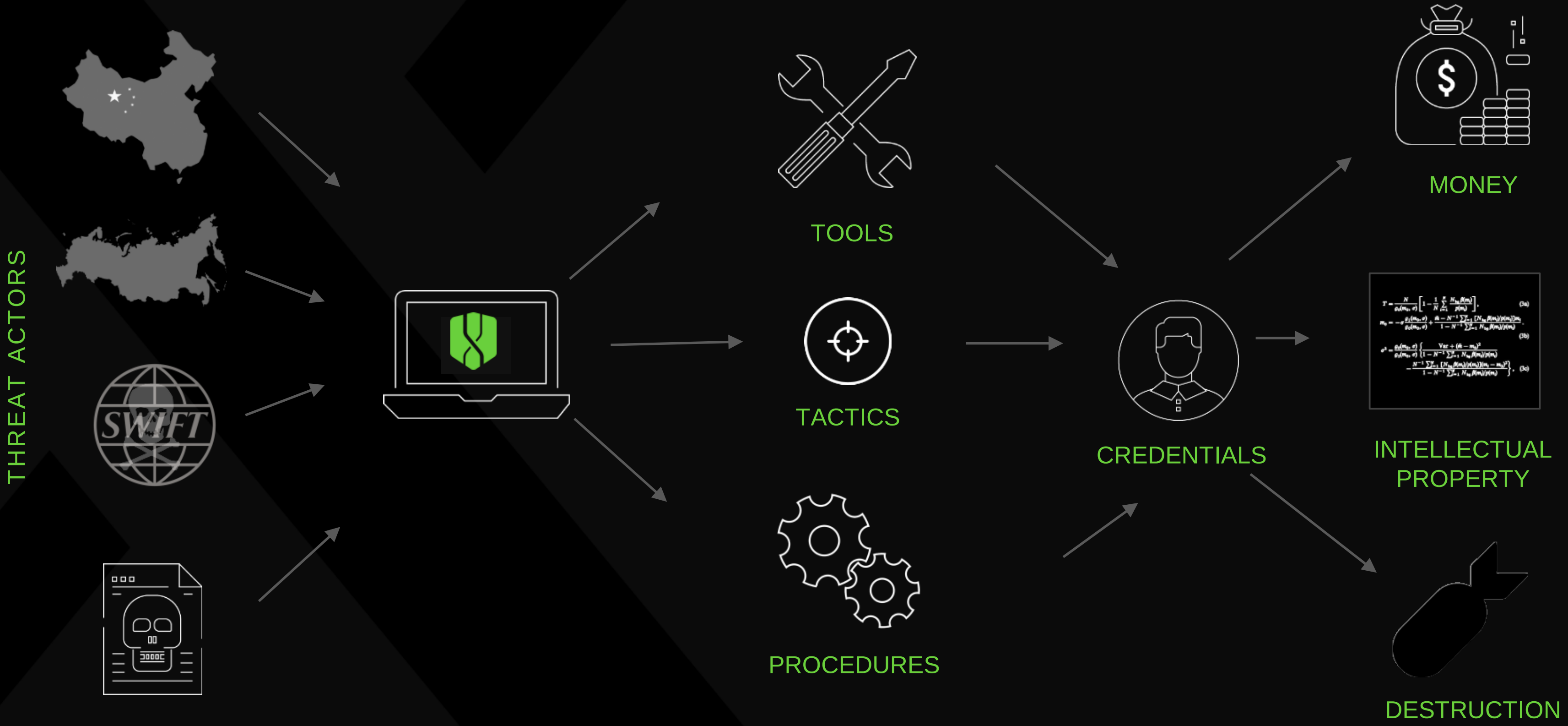
Lateral Movement, Whitelisted Tools, Changing TTPs

Credentials for Compromised User Accounts

Cylance ML for Compromised User Accounts

Data Exfiltration / Sabotage / Ransom

AI vs. All Threats



THREAT ACTORS

TOOLS

TACTICS

PROCEDURES

CREDENTIALS

MONEY

INTELLECTUAL PROPERTY

DESTRUCTION

PREDICTIVE PREVENTION

THE WANNACRY EVOLUTION WILL CONTINUE

PAST

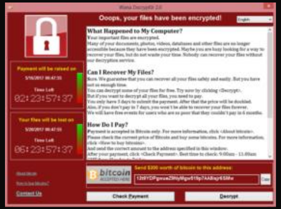
CIRCA 2009
The Lazarus Group – cybercrime group made up of an unknown number of individuals

MARCH 12, 2017
Microsoft patches Windows for known vulnerabilities. **Not everyone updates.**

APRIL 14, 2017
Shadow Brokers dump “Lost in Translation” tools and exploits stolen from the NSA (ExternalBlue)

MAY 11, 2017
EsteemAudit feared to be next zero day exploit utilizing Microsoft RDP

MAY 12, 2017
WannaCry propagates the internet



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
[illegible]

FUTURE

FUTURE
Propagation of variants to WannaCry, ExternalBlue, EsteemAudit…

FUTURE
Destructive malware targeting legacy OSes in critical infrastructure

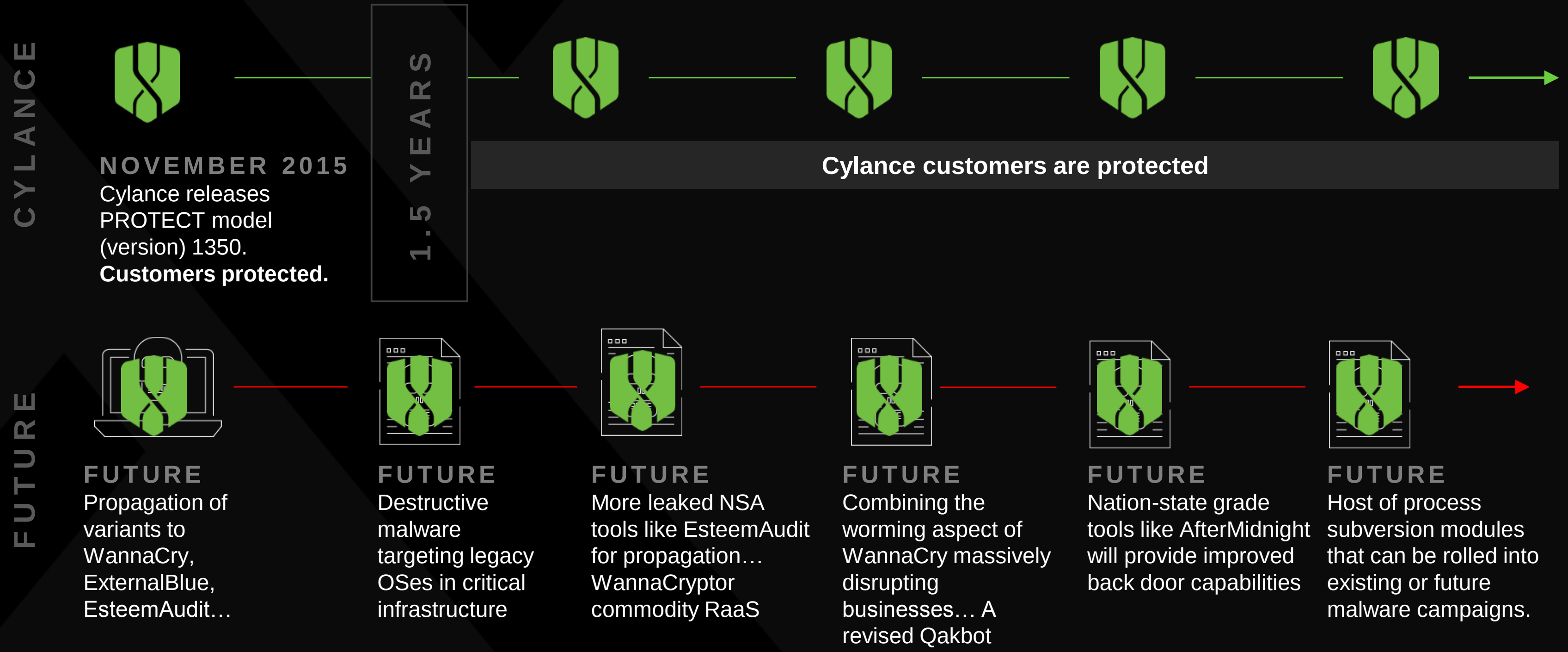
FUTURE
More leaked NSA tools like EsteemAudit for propagation… WannaCryptor commodity RaaS

FUTURE
Combining the worming aspect of WannaCry massively disrupting businesses… A revised Qakbot

FUTURE
Nation-state grade tools like AfterMidnight will provide improved back door capabilities

FUTURE
Host of process subversion modules that can be rolled into existing or future malware campaigns.

CYLANCE PREDICTIVE AI
TEMPORAL PREDICTIVE ADVANTAGE



CYLANCE

NOVEMBER 2015
Cylance releases PROTECT model (version) 1350.
Customers protected.

1.5 YEARS

Cylance customers are protected

FUTURE

FUTURE
Propagation of variants to WannaCry, ExternalBlue, EsteemAudit…

FUTURE
Destructive malware targeting legacy OSes in critical infrastructure

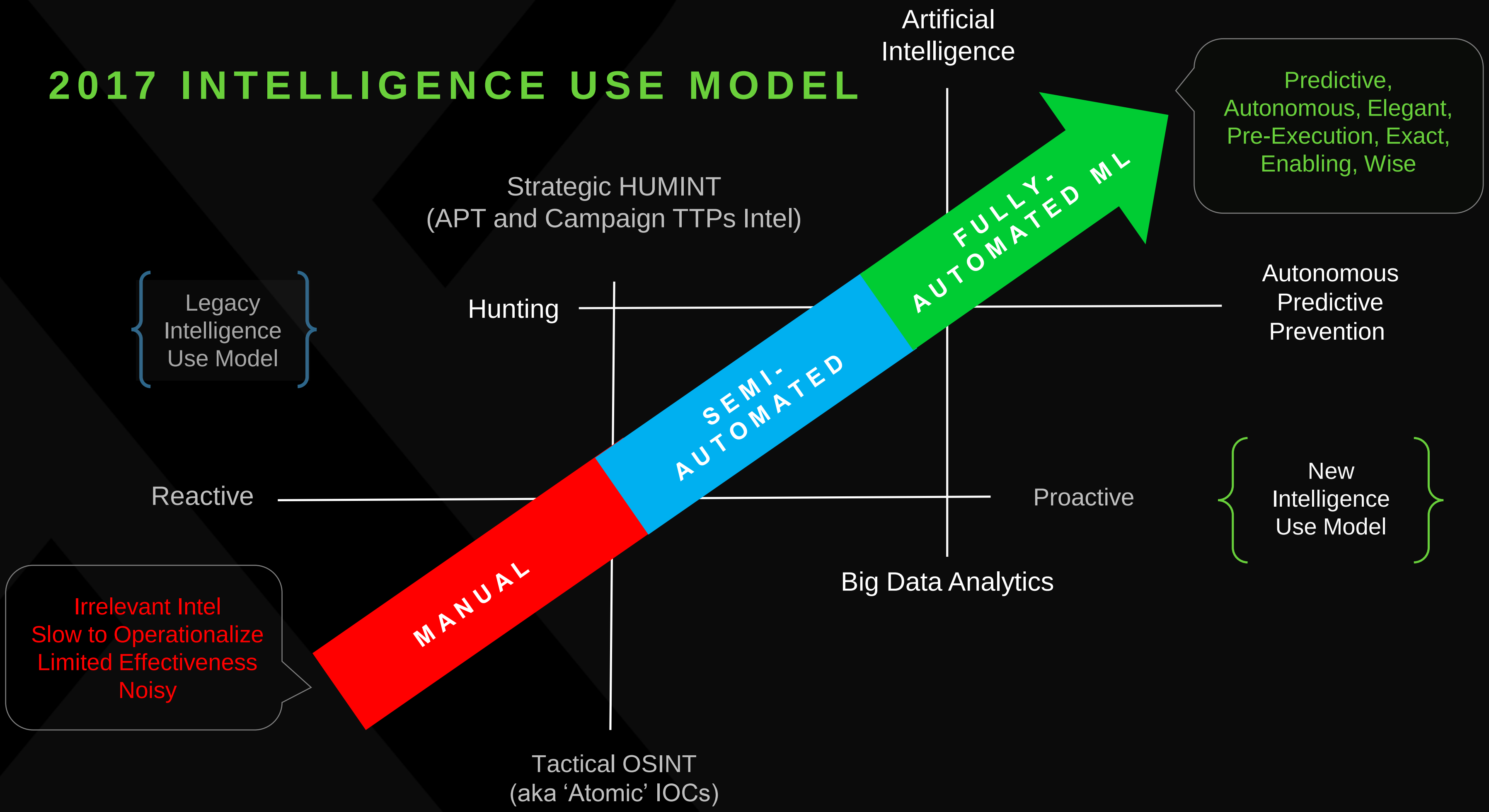
FUTURE
More leaked NSA tools like EsteemAudit for propagation… WannaCryptor commodity RaaS

FUTURE
Combining the worming aspect of WannaCry massively disrupting businesses… A revised Qakbot

FUTURE
Nation-state grade tools like AfterMidnight will provide improved back door capabilities

FUTURE
Host of process subversion modules that can be rolled into existing or future malware campaigns.

2017 INTELLIGENCE USE MODEL



Artificial Intelligence

Predictive, Autonomous, Elegant, Pre-Execution, Exact, Enabling, Wise

Strategic HUMINT
(APT and Campaign TTPs Intel)

Legacy Intelligence Use Model

Hunting

Autonomous Predictive Prevention

FULLY-AUTOMATED ML

SEMI-AUTOMATED

MANUAL

Reactive

Proactive

New Intelligence Use Model

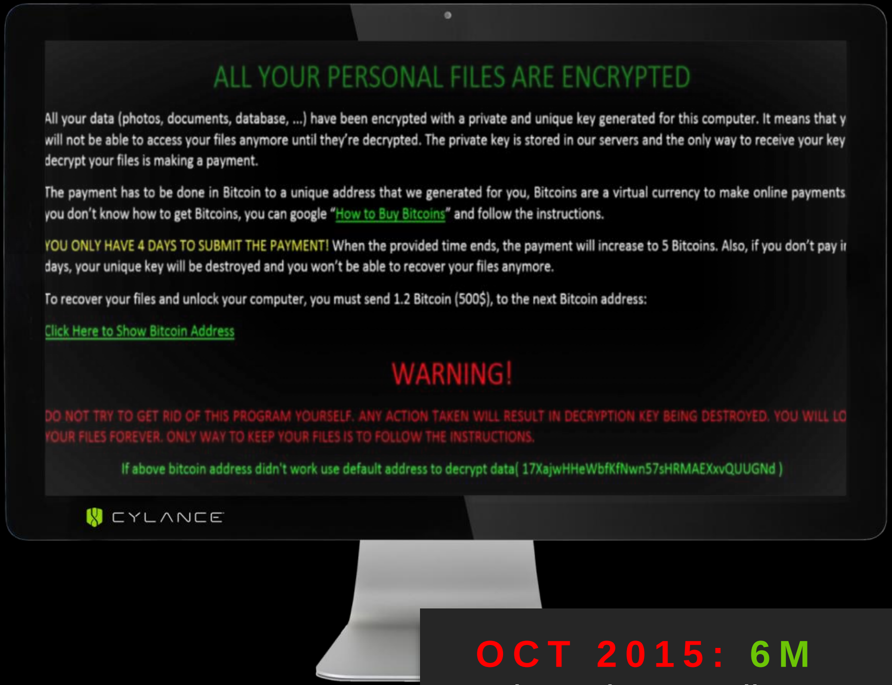
Big Data Analytics

Irrelevant Intel
Slow to Operationalize
Limited Effectiveness
Noisy

Tactical OSINT
(aka ‘Atomic’ IOCs)

ZCRYPTOR –
First appeared late May 2016

- Spear-Phishing
- Fake Installer.exe
- Macros
- USB Drives
- Worm-behavior
- Network Shares
- Bypasses EMET
- Human Discovered April 2016



ALL YOUR PERSONAL FILES ARE ENCRYPTED

All your data (photos, documents, database, ...) have been encrypted with a private and unique key generated for this computer. It means that y will not be able to access your files anymore until they're decrypted. The private key is stored in our servers and the only way to receive your key decrypt your files is making a payment.

The payment has to be done in Bitcoin to a unique address that we generated for you, Bitcoins are a virtual currency to make online payments you don't know how to get Bitcoins, you can google "How to Buy Bitcoins" and follow the instructions.

YOU ONLY HAVE 4 DAYS TO SUBMIT THE PAYMENT! When the provided time ends, the payment will increase to 5 Bitcoins. Also, if you don't pay ir days, your unique key will be destroyed and you won't be able to recover your files anymore.

To recover your files and unlock your computer, you must send 1.2 Bitcoin (500$), to the next Bitcoin address:

Click Here to Show Bitcoin Address

WARNING!

DO NOT TRY TO GET RID OF THIS PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LO YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTIONS.

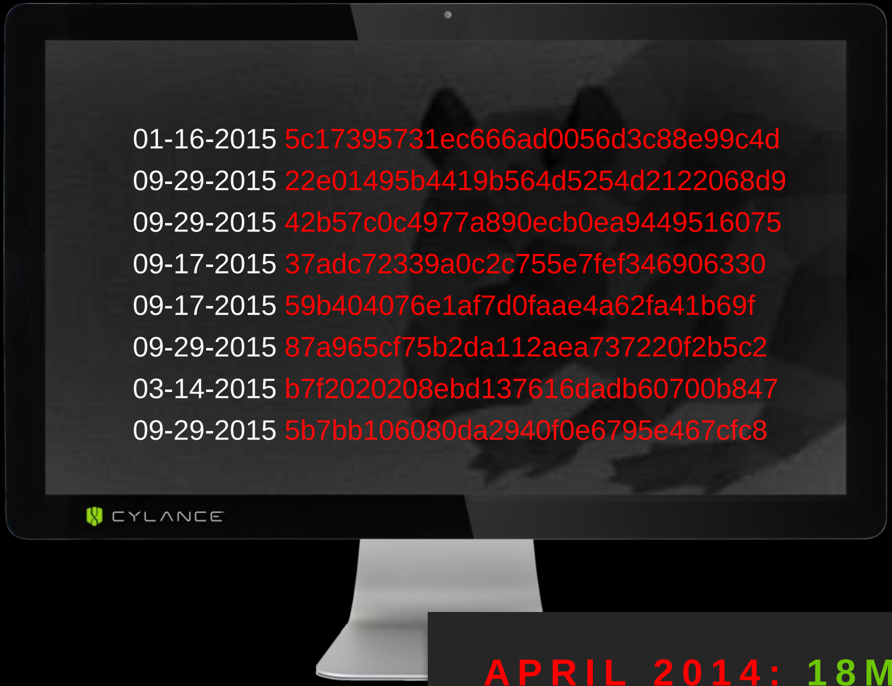
If above bitcoin address didn't work use default address to decrypt data(17XajwHHeWbfKfNwn57sHRMAEXxvQUUGNd)

OCT 2015: 6M
Prior to human discovery

GLASSRAT –

First appeared November 2015

- Espionage RAT
- Undetected for Years
- Human Discovered Nov 23, 2015
- A/V Did not detect new samples
- Detection rates still not high



```
01-16-2015 5c17395731ec666ad0056d3c88e99c4d
09-29-2015 22e01495b4419b564d5254d2122068d9
09-29-2015 42b57c0c4977a890ecb0ea9449516075
09-17-2015 37adc72339a0c2c755e7fef346906330
09-17-2015 59b404076e1af7d0faae4a62fa41b69f
09-29-2015 87a965cf75b2da112aea737220f2b5c2
03-14-2015 b7f2020208ebd137616dadb60700b847
09-29-2015 5b7bb106080da2940f0e6795e467cfc8
```

APRIL 2014: 18M

Prior to human discovery

CYLANCE OPM RESPONSE

- Deployed CylancePROTECT enterprise-wide on 10,000+ systems
- This was a bold move based on risk avoidance (the broader risk to National Security)
- OPM had a legacy A/V deployed that did not detect the intrusions
  - 2,000+ additional pieces of unkown malware predicted and neutralized
- Time from predictive AI detection to full containment and forward-prevention: 10 days