



SECURITY REIMAGINED

IT'S A WHO, NOT A WHAT

WHOAMI

SCOTT.SCHEFERMAN@FIREEYE.COM
SOLUTIONS ARCHITECT



WHYAMI

BECAUSE *THEY'RE* *HERE*



AND...

BECAUSE YOU'RE HERE



AND...

BECAUSE YOU'RE HERE

WHYAMI

BECAUSE *SHE EXISTS*

WHYAMI

BECAUSE SHE EXISTS

WHAT WILL
WE COVER?



WHAT WILL WE COVER?

- They are on *your* Network

WHAT WILL WE COVER?

- They are on *your* Network
- The Myth of Malware

WHAT WILL WE COVER?

- They are on *your* Network
- The Myth of Malware
- Methods of Persistence

WHAT WILL WE COVER?

- They are on *your* Network
- The Myth of Malware
- Methods of Persistence
- It is a *Who*, not a *What*
(*Information vs. Intelligence*)

WHAT WILL WE COVER?

- They are on *your* Network
- The Myth of Malware
- Methods of Persistence
- It is a *Who*, not a *What*
(*Information vs. Intelligence*)
- The New Paradigm

WHY DO WE NEED
A NEW PARADIGM?

WHY DO WE NEED
A NEW PARADIGM?

BECAUSE
WE NEED
TO WIN

LET'S GET THIS OUT OF THE WAY, SHALL WE?



LET'S GET THIS OUT OF THE WAY, SHALL WE?



LET'S GET THIS OUT OF THE WAY, SHALL WE?

THE THREAT ACTORS ARE
ALREADY IN YOUR NETWORK

AND YES, EVEN IN STATE AND LOCAL
GOVERNMENT NETWORKS...

May 1 2014 - May 1 2015

AND YES, EVEN IN STATE AND LOCAL GOVERNMENT NETWORKS...

May 1 2014 - May 1 2015

130

of S&L
POVs

AND YES, EVEN IN STATE AND LOCAL GOVERNMENT NETWORKS...

May 1 2014 - May 1 2015

130

of S&L
POVs

95

% Compromised

AND YES, EVEN IN STATE AND LOCAL GOVERNMENT NETWORKS...

May 1 2014 - May 1 2015

130

of S&L
POVs

95

% Compromised

21

% with
APT Activity

AND YES, EVEN IN STATE AND LOCAL
GOVERNMENT NETWORKS...

May 1 2014 - May 1 2015

AND YES, EVEN IN STATE AND LOCAL
GOVERNMENT NETWORKS...

May 1 2014 - May 1 2015

23

Ave # Hosts

Pwnd

AND YES, EVEN IN STATE AND LOCAL GOVERNMENT NETWORKS...

May 1 2014 - May 1 2015

23

Ave # Hosts
Pwnd

37

Ave # Unique
Call-Backs

AND YES, EVEN IN STATE AND LOCAL GOVERNMENT NETWORKS...

May 1 2014 - May 1 2015

23

Ave # Hosts
Pwnd

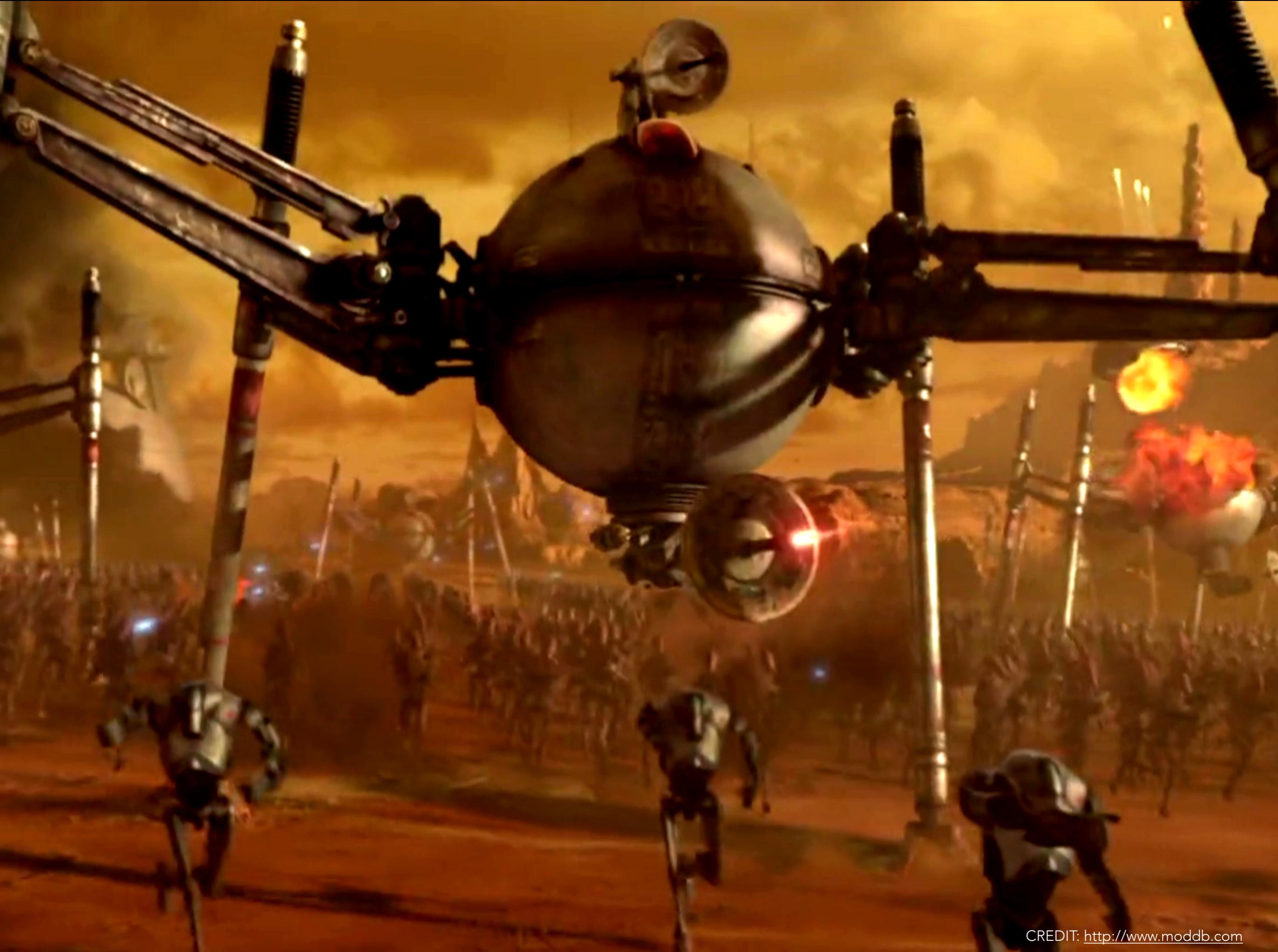
37

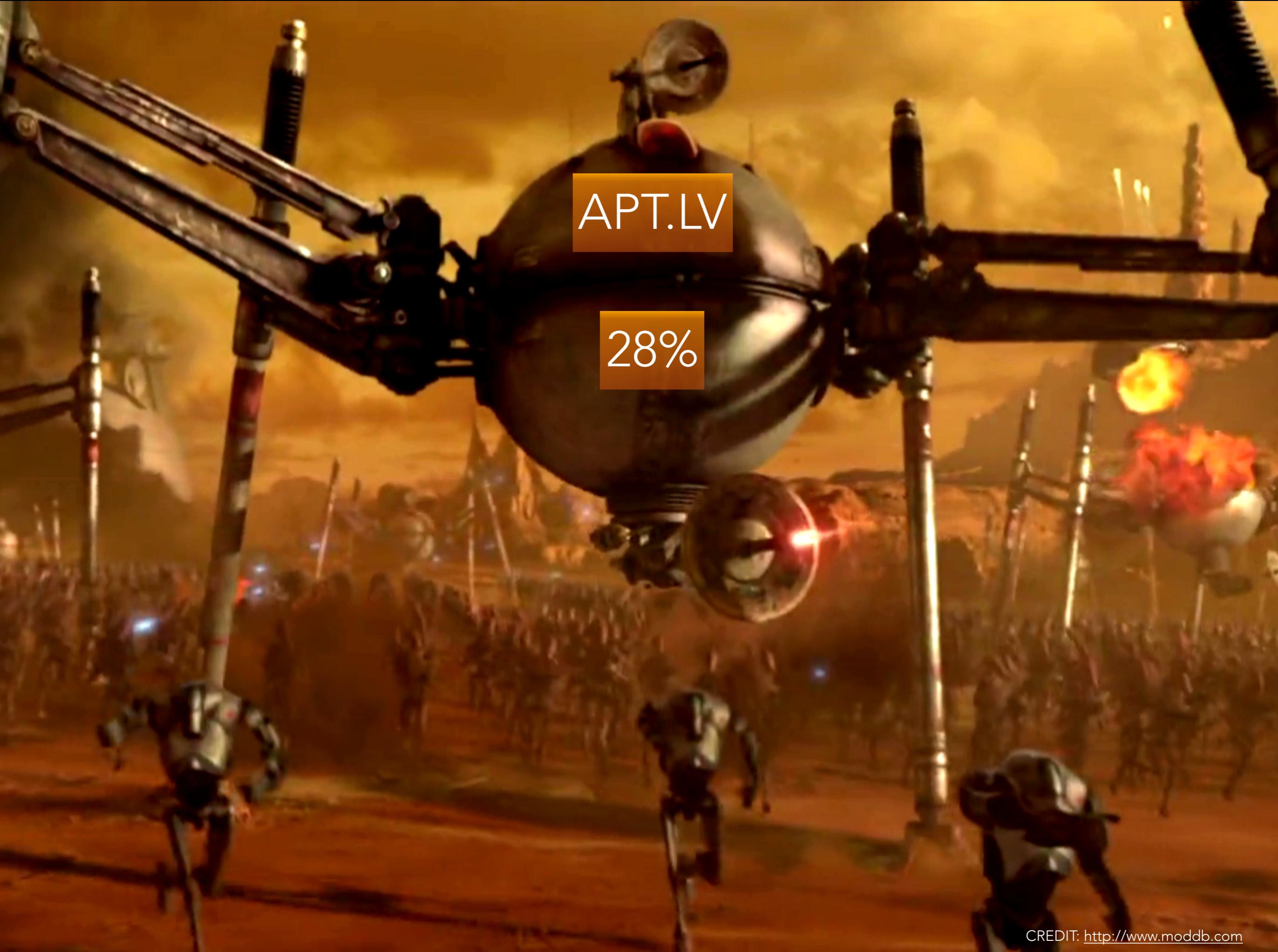
Ave # Unique
Call-Backs

177

Ave # of Malware
Downloaded

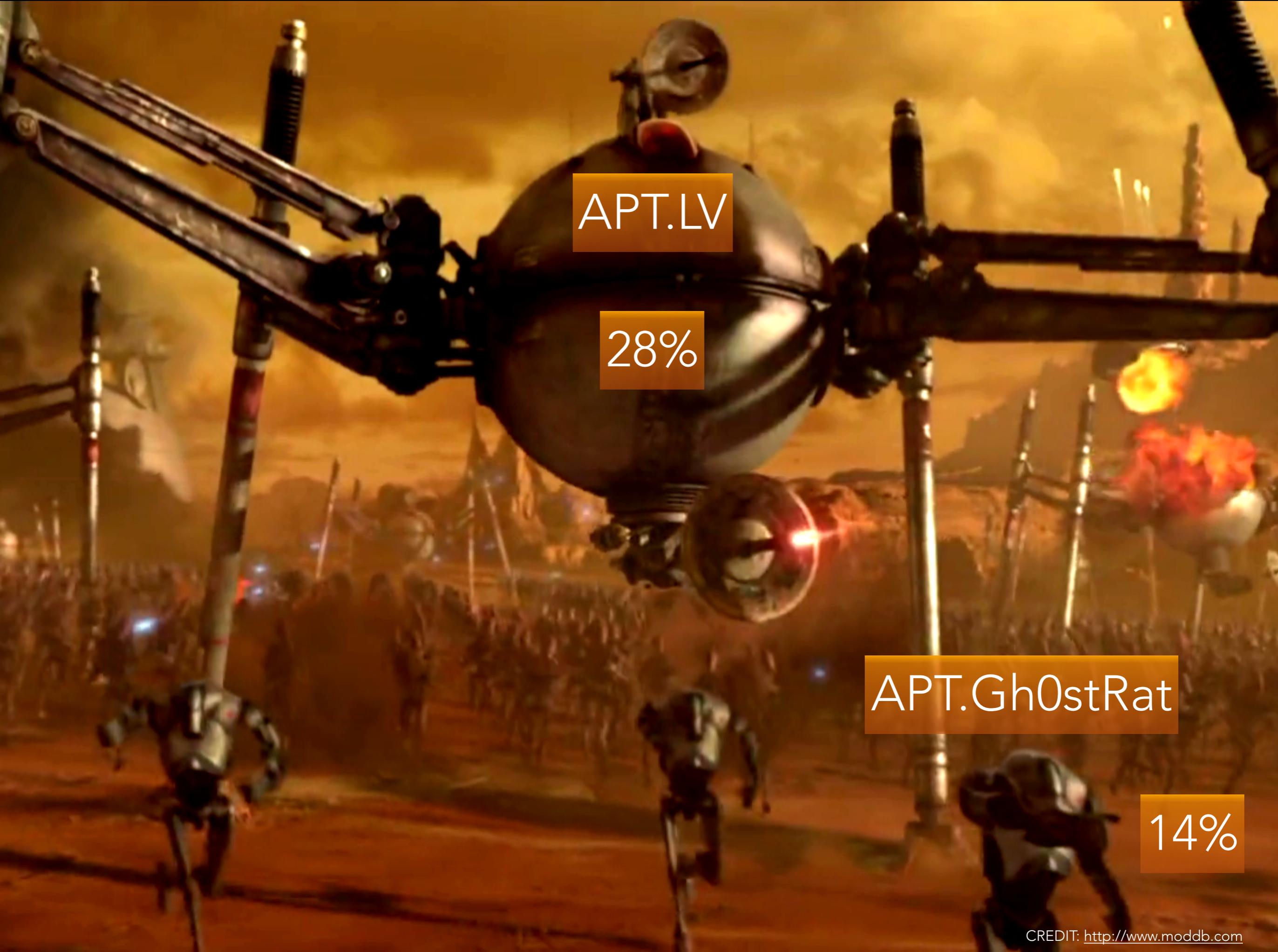
SO WHAT DOES THIS ACTUALLY
LOOK LIKE ON *YOUR NETWORK?*





APT.LV

28%



APT.LV

28%

APT.Gh0stRat

14%

APT.LV

28%

```
lv|'|  
2YLZgNin2KrZgNmEINmF2YDYo  
9is2YDZi  
NixXzQwMENEw|'|Remote  
PC|'|admin|'| 2013-04-22|'|  
USA|'|Win XP Professional SP2  
x86|'| |'|0.5.0E|'|.|'|  
QzpcV0IORE9XU1xzeXN0ZW0zM  
lxjbWQuZXhl |'|[endof]
```

APT.LV

28%

```
lv'|'  
2YLZgNin2KrZgNmEINmF2YDYo  
9is2YDZi  
NixXzQwMENEw'|'|Remote  
PC'|'|admin'|'| 2013-04-22'|'|  
USA'|'|Win XP Professional SP2  
x86'|'| '|'|0.5.0E'|'|.'|'|  
QzpcV0IORE9XU1xzeXN0ZW0zM  
lxjbWQuZXhl '|'|[endof]
```

Download more malware
Remote Desktop Access
Conduct deeper network reconnaissance
Search for specific files or information
Access software/hardware management controls
Exfiltrate stolen data, log keystrokes

APT.LV

28%

```
lv'|'  
2YLZgNin2KrZgNmEINmF2YDYo  
9is2YDZi  
NixXzQwMENEw'|'|Remote  
PC'|'|admin'|'| 2013-04-22'|'|  
USA'|'|Win XP Professional SP2  
x86'|'| YES '|'|0.5.0E'|'|. '|'|  
QzpcV0IORE9XU1xzeXN0ZW0zM  
lxjbWQuZXhl '|'|[endof]
```

Download more malware
Remote Desktop Access
Conduct deeper network reconnaissance
Search for specific files or information
Access software/hardware management controls
Exfiltrate stolen data, log keystrokes

APT.LV

28%

```
lv'|'  
2YLZgNin2KrZgNmEINmF2YDYo  
9is2YDZi  
NixXzQwMENEw'|'|Remote  
PC'|'|admin'|'| 2013-04-22'|'|  
USA'|'|Win XP Professional SP2  
x86'|'| YES '|'|0.5.0E'|'|. '|'|  
QzpcV0IORE9XU1xzeXN0ZW0zM  
lxjbWQuZXhl '|'|[endof]
```

Download more malware
Remote Desktop Access
Conduct deeper network reconnaissance
Search for specific files or information
Access software/hardware management controls
Exfiltrate stolen data, log keystrokes

Do You Want To
Open TROJAN.EXE?

APT.LV

28%

```
lv'|'  
2YLZgNin2KrZgNmEINmF2YDYo  
9is2YDZi  
NixXzQwMENEw'|'|Remote  
PC'|'|admin'|'| 2013-04-22'|'|  
USA'|'|Win XP Professional SP2  
x86'|'| YES '|'|0.5.0E'|'|. '|'|  
QzpcV0IORE9XU1xzeXN0ZW0zM  
lxjbWQuZXhl '|'|[endof]
```

Download more malware
Remote Desktop Access
Conduct deeper network reconnaissance
Search for specific files or information
Access software/hardware management
controls
Exfiltrate stolen data, log keystrokes



APT.Gh0stRat

14%

APT1
APT10
APT12
APT14
APT16
APT17
APT18
APT21
APT23
APT27
APT4
APT5
APT9

APT.Gh0stRat

14%

APT1
APT10
APT12
APT14
APT16
APT17
APT18
APT21
APT23
APT27
APT4
APT5
APT9



APT.Gh0stRat

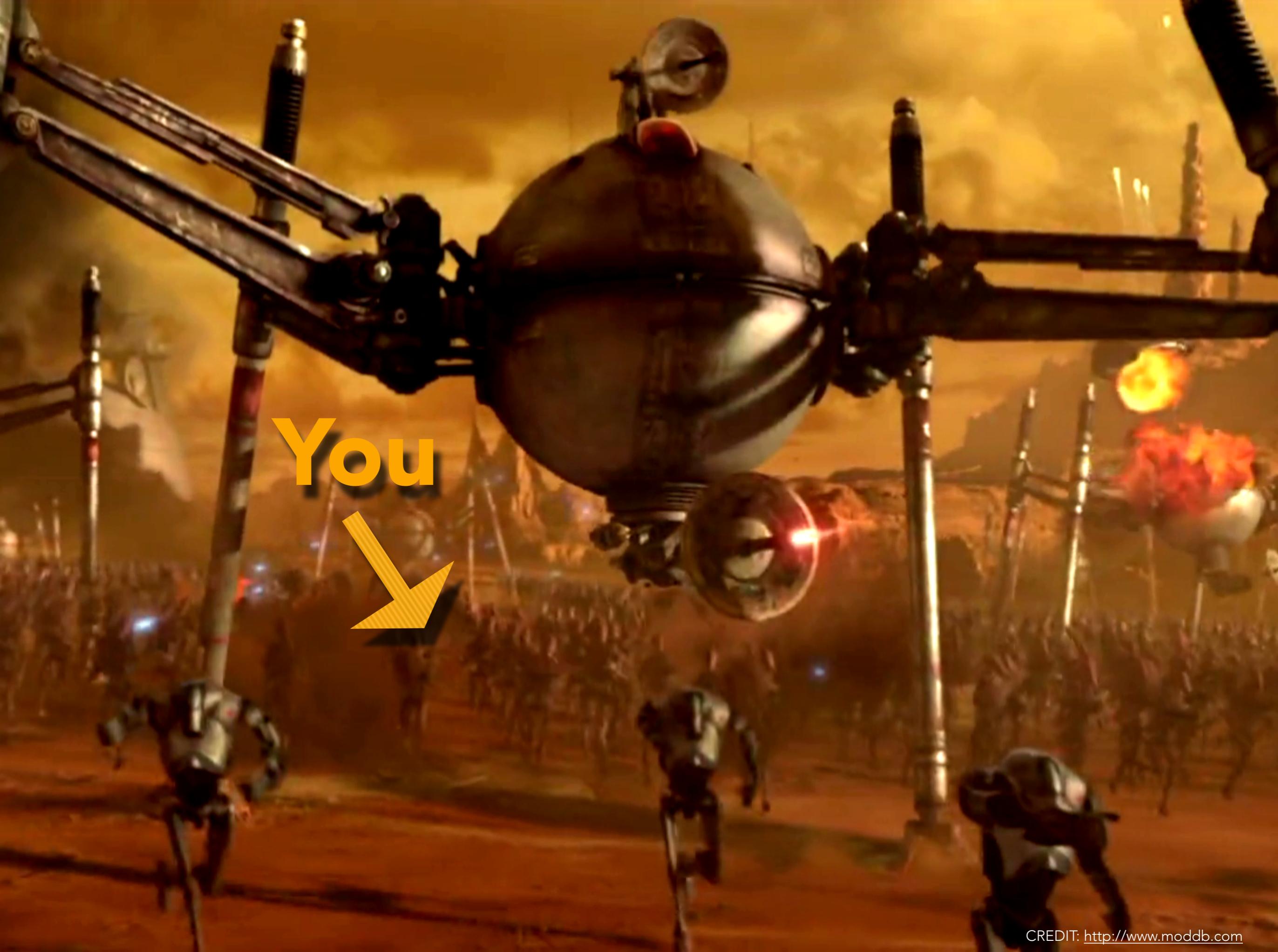
14%





You





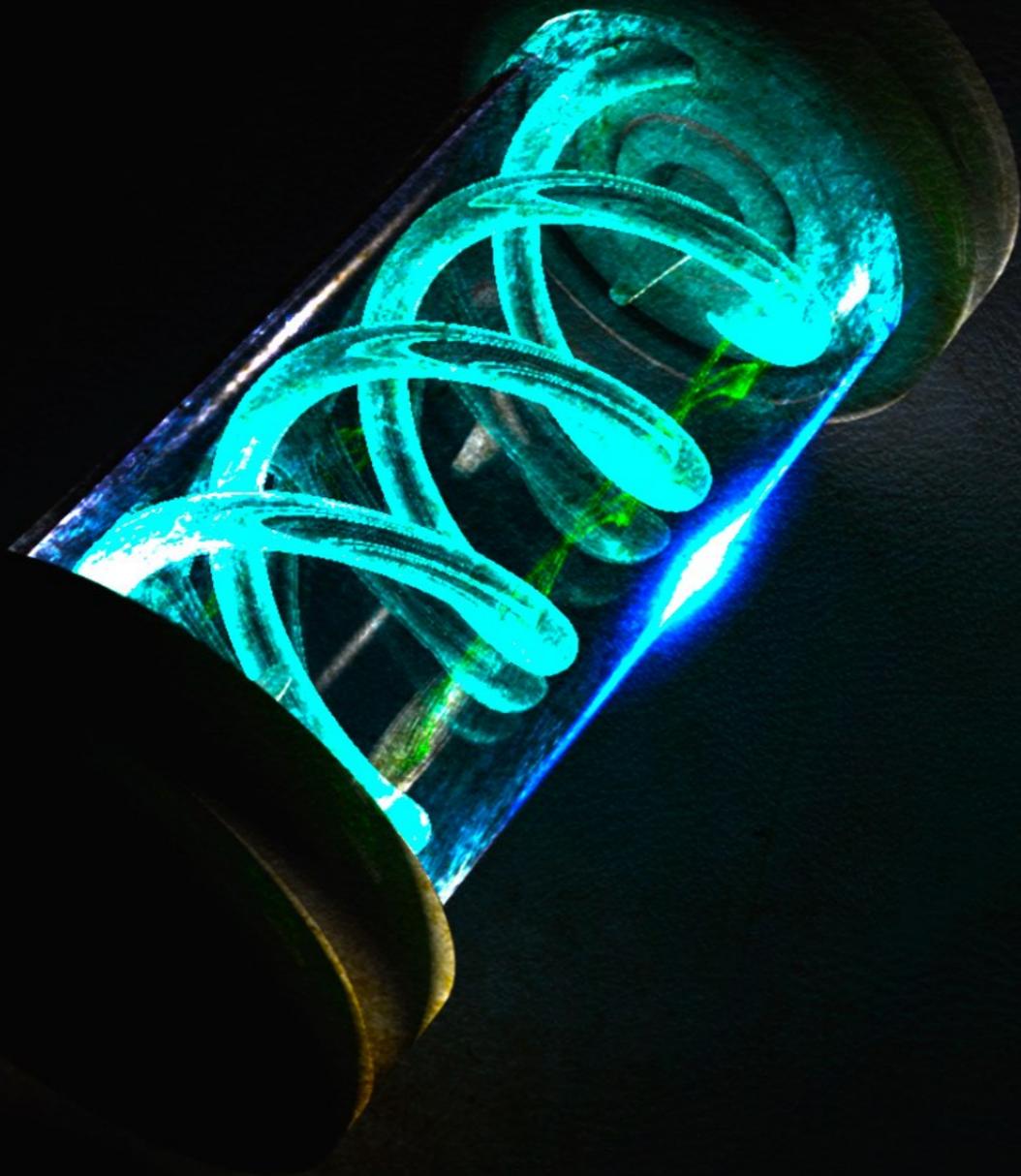
You



SO NOW LET'S TALK
ABOUT THIS MALWARE

70-90% of Malware Samples are Unique to a Given
Organization

70-90% of Malware Samples are Unique to a Given Organization



70-90% of Malware Samples are Unique to a Given Organization



= Malware **NOISE**

The Real Deal?

TRDEALMGN4UVM42G.ONION

Adobe Flash < 16.0.0.296 (CVE-2015-0313) **BTC 2.50000000**

Adobe flash exploit for versions > 16.0.0.296 made 100 FUD. Tested on windows 7 with IE.

Message

Purchase

You can ask for demo in PM but that is what escrow is here to prevent :)

By [bestbuy \(0\)](#)

Added: 31 March 2015

☆☆☆☆☆ 0 reviews

FUD .js download and execute **BTC 1.30000000**

100 FUD .js file for download and execute, just attach, send and wait ;)

Message

Purchase

You can ask for demo in PM but that is why you have escrow...

By [bestbuy \(0\)](#)

Added: 1 April 2015

☆☆☆☆☆ 0 reviews

Available Locations	Cost
Worldwide	BTC 0.00300000

The real GovRAT **BTC 4.50000000**

100 percent FUD - Tested with the strictest firewall policies and AV rules.

Message

Purchase

You are buying the source code + Instructions on setup and compile + 1 digital certificate for code signing to sign your files.

Functions:

- [*] Access C&C with any browser.
- [*] Compile C&C for Linux OR Windows.
- [*] VALID Digital signature for binary files - alone worth \$1000.
- [*] Cannot be reversed without the private key. Oday anti-debugging.
- [*] Automatically maps all hard disks and network disks.
- [*] Creates a map of files to browse even when the target is offline.
- [*] Execute commands remotely.
- [*] Upload files or Upload and Execute files to target.
- [*] Download files from target. All files are compressed with LZMA for faster downloads.
- [*] Customized encryption for communications.
- [*] SSL Support for communications. (you have to get your own certificate).

The Real Deal?

TRDEALMGN4UVM42G.ONION

Adobe Flash < 16.0.0.296 (CVE-2015-0313) **BTC 2.50000000**

Adobe flash exploit for versions > 16.0.0.296 made 100 FUD. Tested on windows 7 with IE.

Message
Purchase

You can ask for demo in PM but that is what escrow is here to prevent :)

By [bestbuy](#) (0)

Added: 31 March 2015

☆☆☆☆☆ 0 reviews

FUD .js download and execute **BTC 1.30000000**

100 FUD .js file for download and execute, just attach, send and wait ;)

Message
Purchase

You can ask for demo in PM but that is why you have escrow...

By [bestbuy](#) (0)

Added: 1 April 2015

☆☆☆☆☆ 0 reviews

Available Locations	Cost
Worldwide	BTC 0.00300000

The real GovRAT **BTC 4.50000000**

100 percent FUD - Tested with the strictest firewall policies and AV rules.

Message
Purchase

You are buying the source code + Instructions on setup and compile + 1 digital certificate for code signing to sign your files.

Functions:

- [*] Access C&C with any browser.
- [*] Compile C&C for Linux OR Windows.
- [*] VALID Digital signature for binary files - alone worth \$1000.
- [*] Cannot be reversed without the private key. Oday anti-debugging.
- [*] Automatically maps all hard disks and network disks.
- [*] Creates a map of files to browse even when the target is offline.
- [*] Execute commands remotely.
- [*] Upload files or Upload and Execute files to target.
- [*] Download files from target. All files are compressed with LZMA for faster downloads.
- [*] Customized encryption for communications.
- [*] SSL Support for communications. (you have to get your own certificate).

FUD?

FUD?

FUD?

The Real Deal?

TRDEALMGN4UVM42G.ONION

Adobe Flash < 16.0.0.296 (CVE-2015-0313) BTC 2.50000000

Adobe flash exploit for versions > 16.0.0.296 made 100 FUD. Tested on windows 7 with IE.

Message
Purchase

You can ask for demo in PM but that is what escrow is here to prevent :)

By [bestbuy](#) (0)

Added: 31 March 2015

☆☆☆☆☆ 0 reviews

FUD .js download and execute BTC 1.30000000

100 FUD .js file for download and execute, just attach, send and wait ;)

Message
Purchase

You can ask for demo in PM but that is why you have escrow...

By [bestbuy](#) (0)

Added: 1 April 2015

☆☆☆☆☆ 0 reviews

Available Locations	Cost
Worldwide	BTC 0.00300000

The real GovRAT BTC 4.50000000

100 percent FUD - Tested with the strictest firewall policies and AV rules.

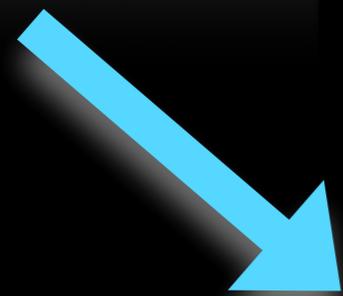
Message
Purchase

You are buying the source code + Instructions on setup and compile + 1 digital certificate for code signing to sign your files.

Functions:

- [*] Access C&C with any browser.
- [*] Compile C&C for Linux OR Windows.
- [*] VALID Digital signature for binary files - alone worth \$1000.
- [*] Cannot be reversed without the private key. Oday anti-debugging.
- [*] Automatically maps all hard disks and network disks.
- [*] Creates a map of files to browse even when the target is offline.
- [*] Execute commands remotely.
- [*] Upload files or Upload and Execute files to target.
- [*] Download files from target. All files are compressed with LZMA for faster downloads.
- [*] Customized encryption for communications.
- [*] SSL Support for communications. (you have to get your own certificate).

FUD?



FUD?



FUD?



The Real Deal?

TRDEALMGN4UVM42G.ONION

Adobe Flash < 16.0.0.296 (CVE-2015-0313) BTC 2.50000000

Adobe flash exploit for versions > 16.0.0.296 made 100 FUD. Tested on windows 7 with IE.

Message
Purchase

You can ask for demo in PM but that is what escrow is here to prevent :)

By [bestbuy](#) (0)

Added: 31 March 2015

☆☆☆☆☆ 0 reviews

FUD .js download and execute BTC 1.30000000

100 FUD .js file for download and execute, just attach, send and wait ;)

Message
Purchase

You can ask for demo in PM but that is why you have escrow...

By [bestbuy](#) (0)

Added: 1 April 2015

☆☆☆☆☆ 0 reviews

Available Locations	Cost
Worldwide	BTC 0.00300000

The real GovRAT BTC 4.50000000

100 percent FUD - Tested with the strictest firewall policies and AV rules.

Message
Purchase

You are buying the source code + Instructions on setup and compile + 1 digital certificate for code signing to sign your files.

Functions:

- [*] Access C&C with any browser.
- [*] Compile C&C for Linux OR Windows.
- [*] VALID Digital signature for binary files - alone worth \$1000.
- [*] Cannot be reversed without the private key. Oday anti-debugging.
- [*] Automatically maps all hard disks and network disks.
- [*] Creates a map of files to browse even when the target is offline.
- [*] Execute commands remotely.
- [*] Upload files or Upload and Execute files to target.
- [*] Download files from target. All files are compressed with LZMA for faster downloads.
- [*] Customized encryption for communications.
- [*] SSL Support for communications. (you have to get your own certificate).

v2.scan.majyx.net

35 AV SCANNERS

FUD?

FUD?

FUD?



If Time Were a Spear

AND MALWARE WERE THE PROBLEM

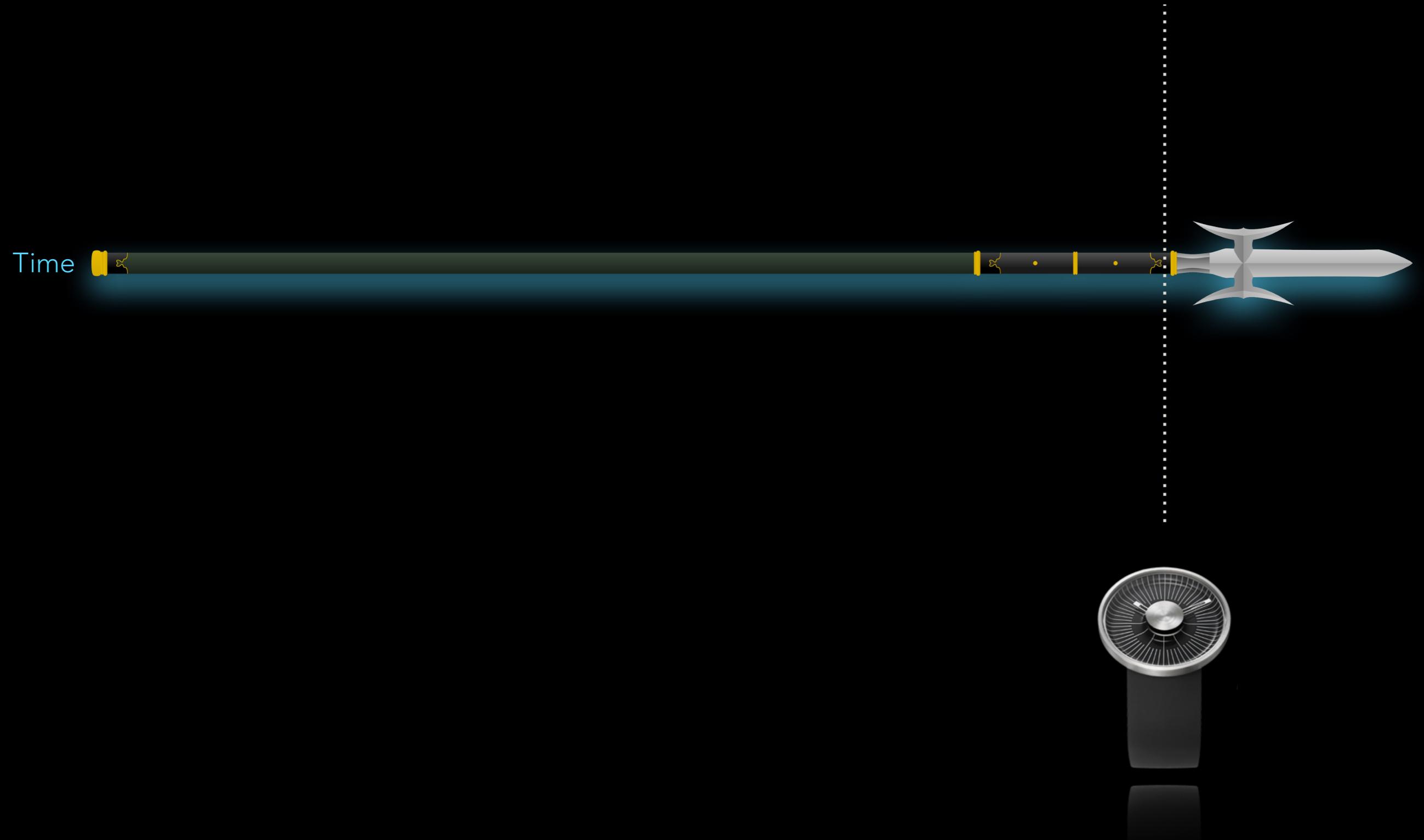
If Time Were a Spear

AND MALWARE WERE THE PROBLEM



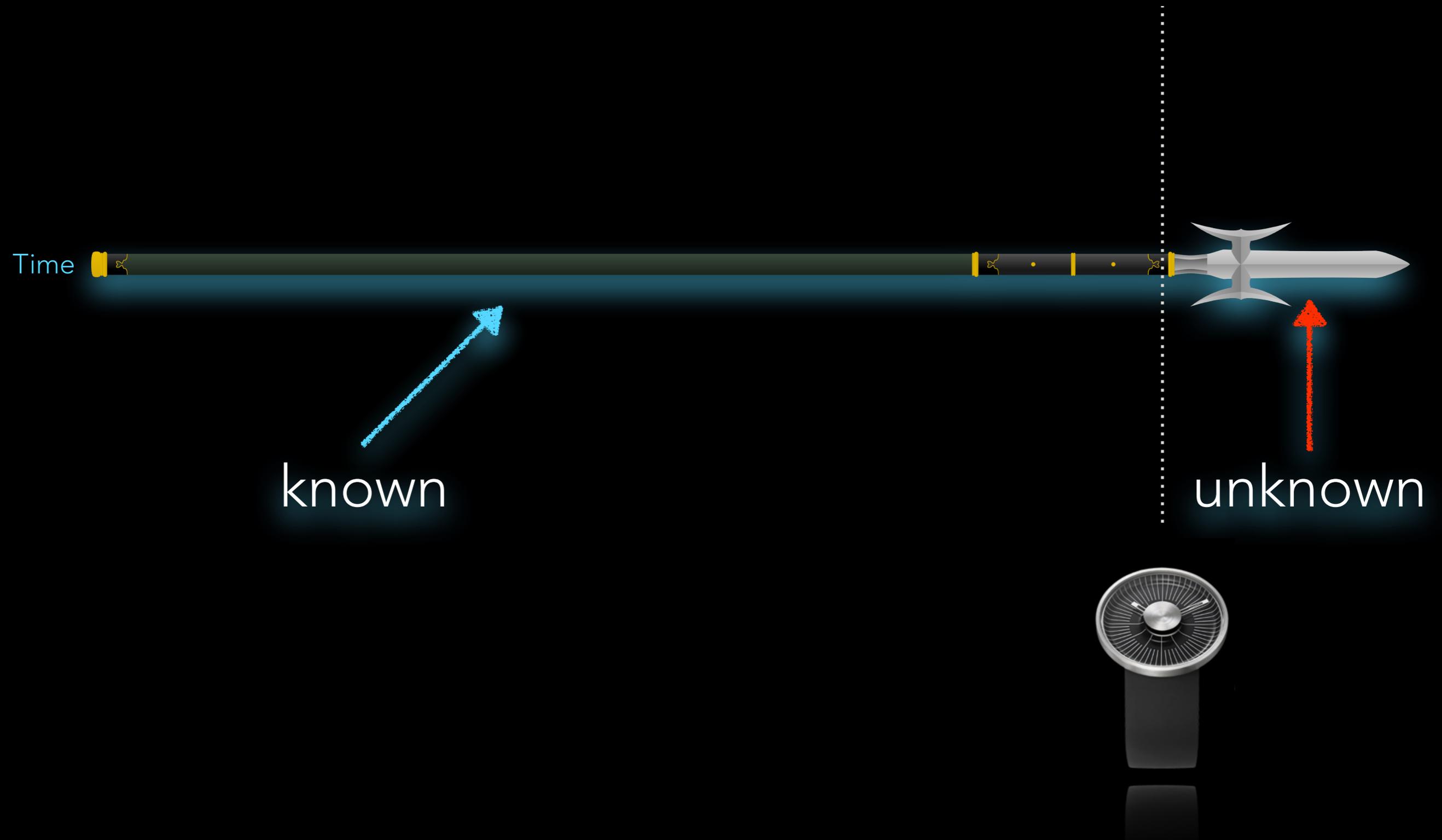
If Time Were a Spear

AND MALWARE WERE THE PROBLEM



If Time Were a Spear

AND MALWARE WERE THE PROBLEM



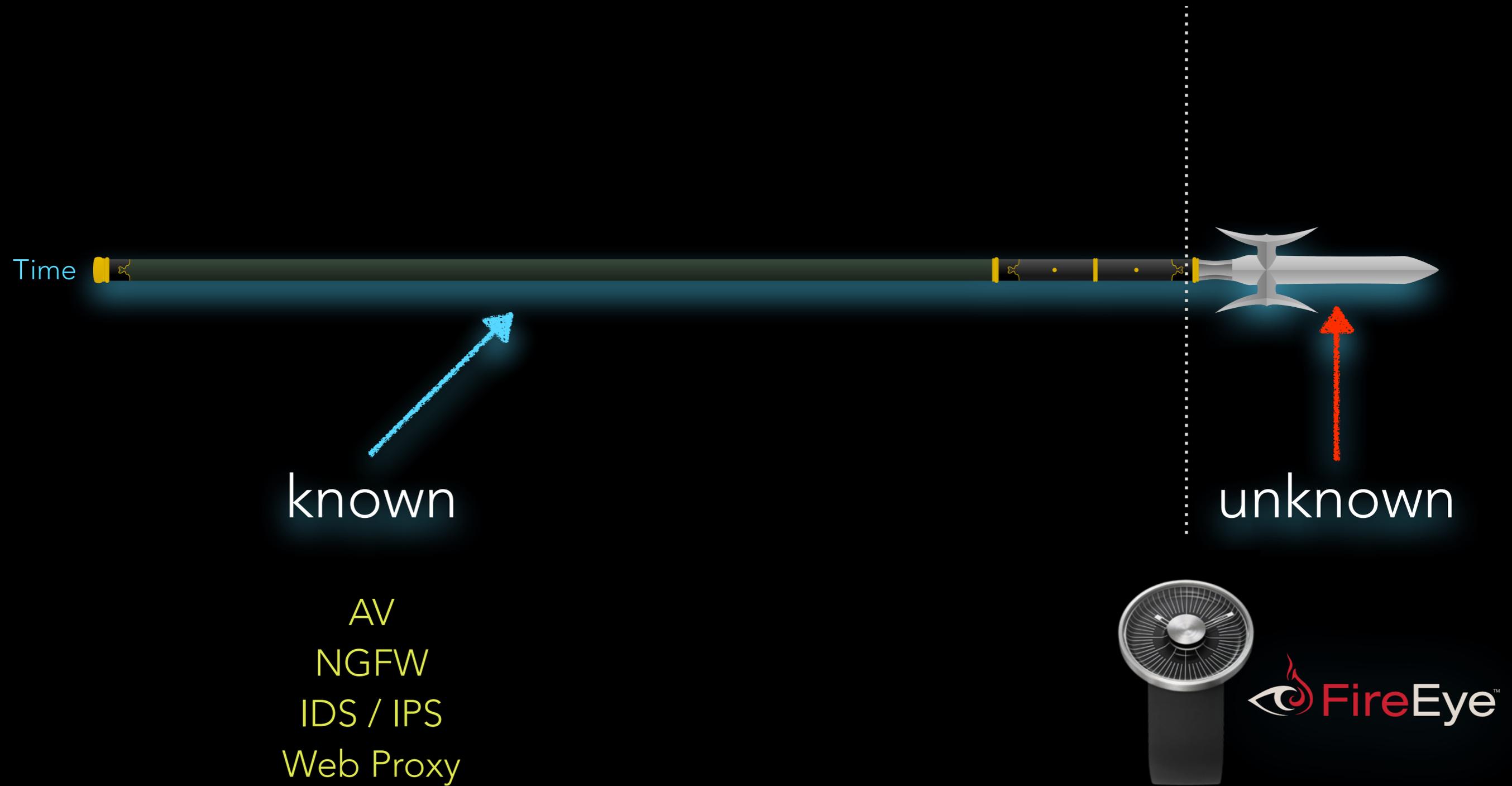
If Time Were a Spear

AND MALWARE WERE THE PROBLEM



If Time Were a Spear

AND MALWARE WERE THE PROBLEM



BUT MALWARE IS NOT
THE PROBLEM

Malware doesn't Compromise People...

People Compromise People

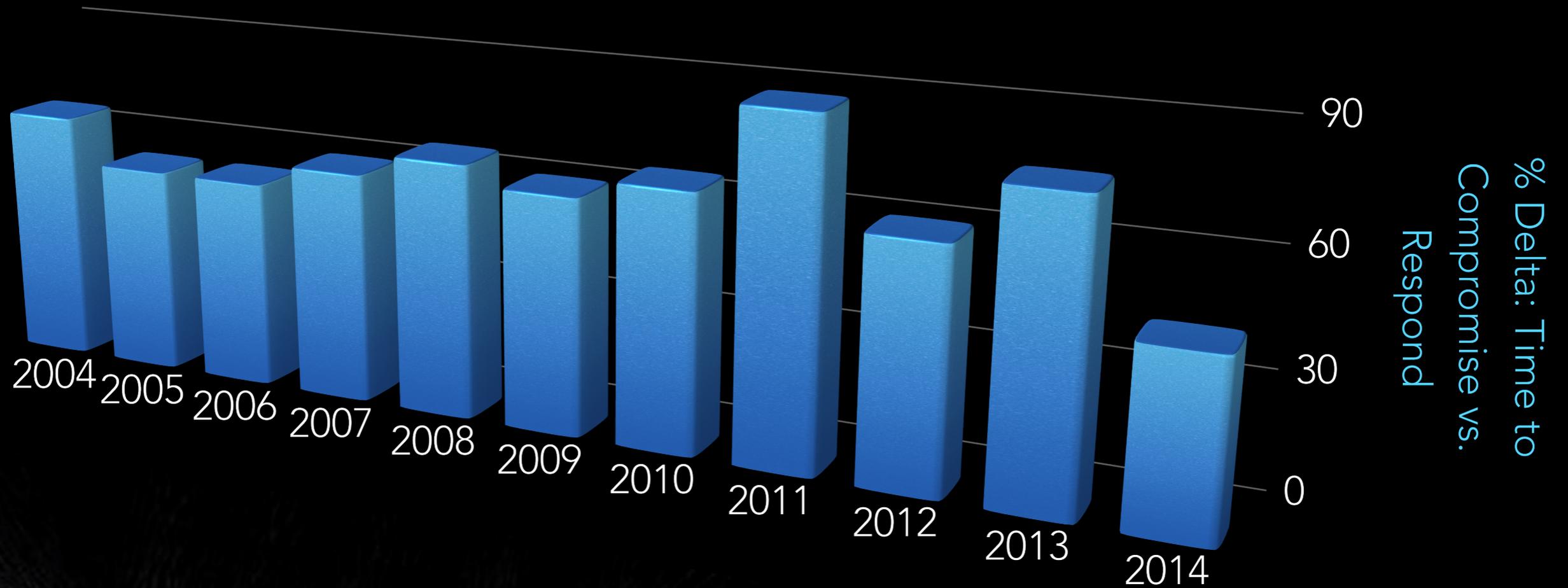
**46% OF COMPROMISED HOSTS
HAVE ONE THING IN COMMON:
NO MALWARE**



**100% OF BREACHES INVOLVED
STOLEN CREDENTIALS**

THE DETECTION DEFICIT TREND

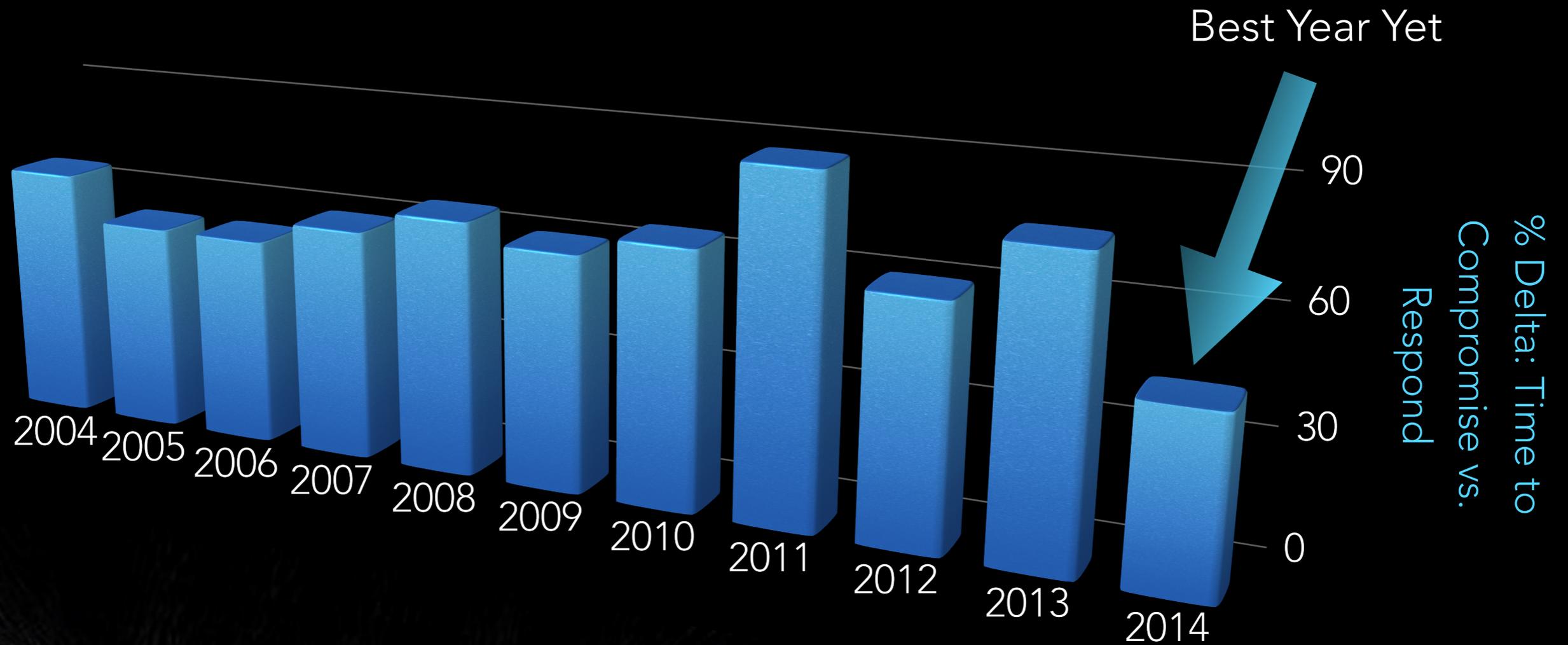
CAT VS. MOUSE



(REF: VERIZON DBIR 2015)

THE DETECTION DEFICIT TREND

CAT VS. MOUSE

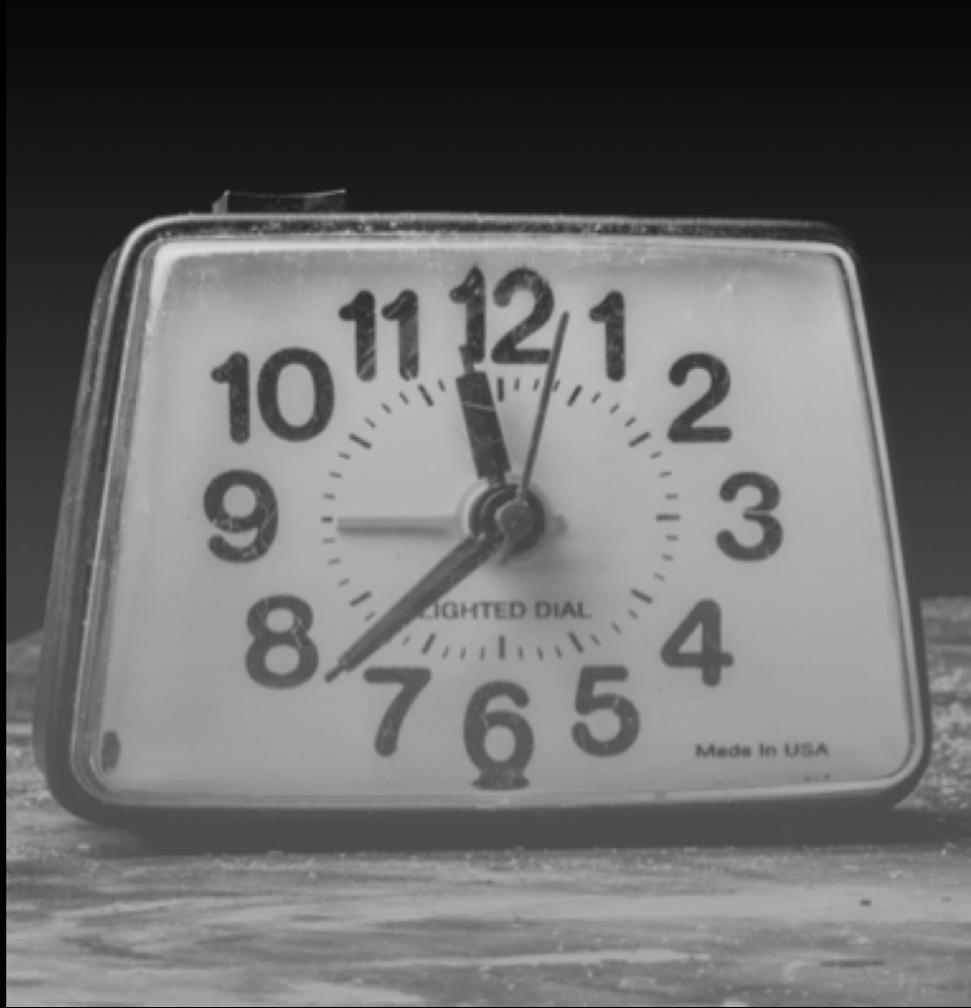


(REF: VERIZON DBIR 2015)

SPEAKING OF TIME

DWELL TIME = 205 DAYS

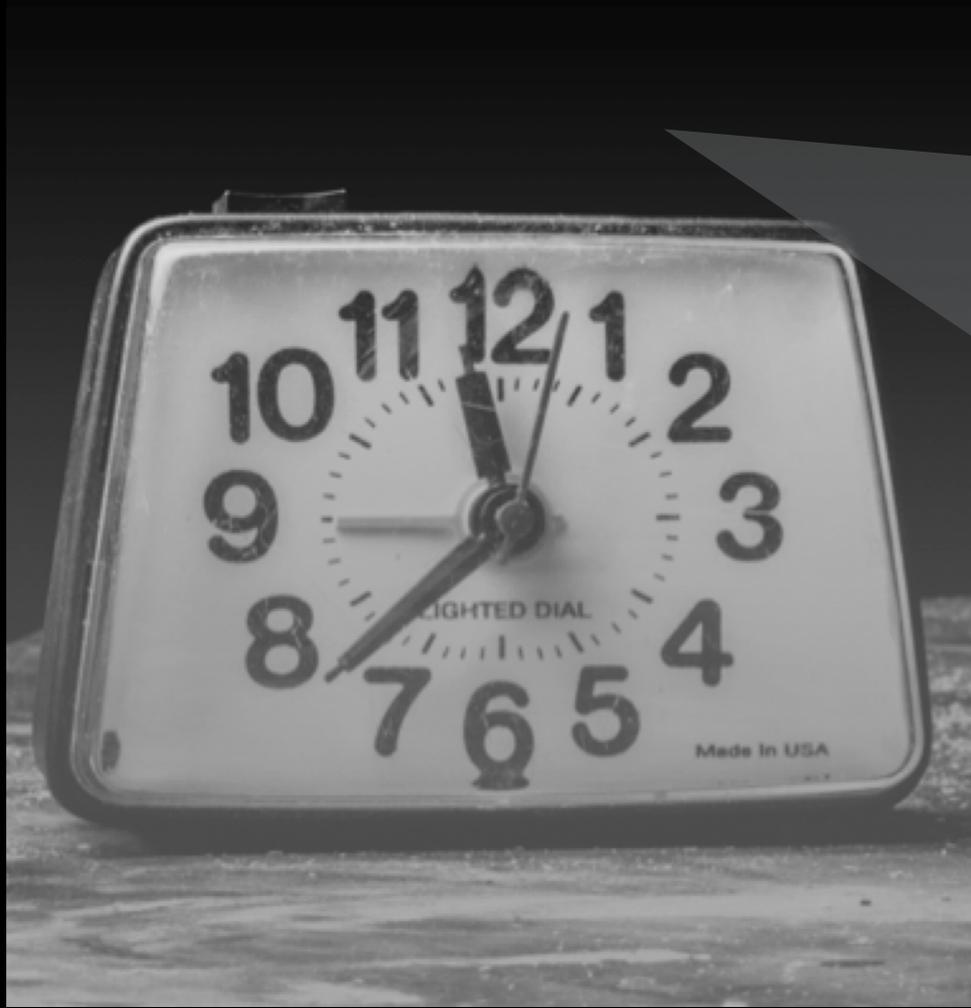
MEDIAN # DAYS ATTACKERS WERE ON SYSTEM BEFORE DETECTION



SPEAKING OF TIME

DWELL TIME = 205 DAYS

MEDIAN # DAYS ATTACKERS WERE ON SYSTEM BEFORE DETECTION

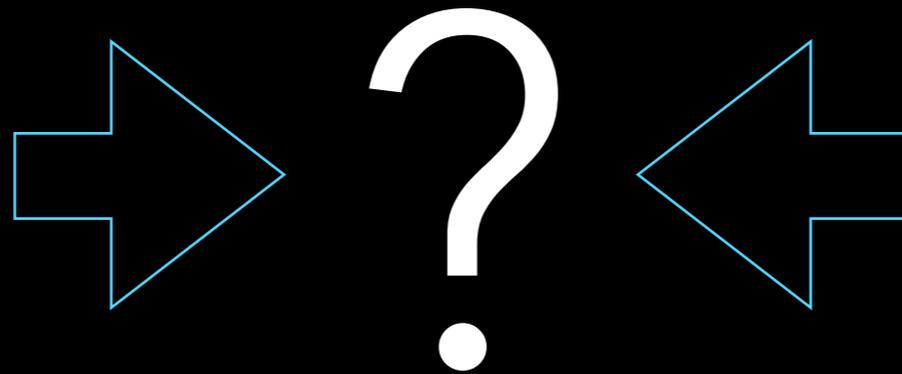


APT30
10 Years in
Air-Gapped
Networks!

AS EARLY AS 2009, GHOSTNET (GHOSTRAT'S EXPLOIT/DROPPER NETWORK) HAD ALREADY INFILTRATED AT LEAST **1,295** COMPUTERS IN **103** COUNTRIES **30%** OF WHICH WERE **HIGH-VALUE TARGETS**, INCLUDING MINISTRIES OF FOREIGN AFFAIRS, EMBASSIES, INTERNATIONAL ORGANIZATIONS, NEWS MEDIA, AND NGOS.

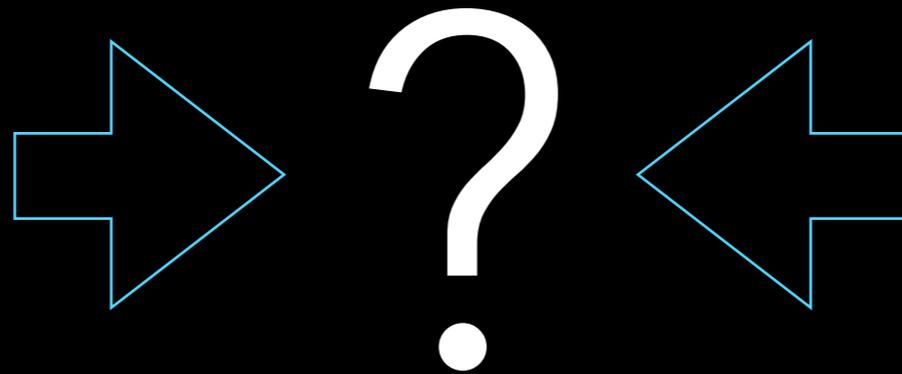
BEFORE ANYONE HAD
DETECTED IT...

CYBER THREAT INTELLIGENCE



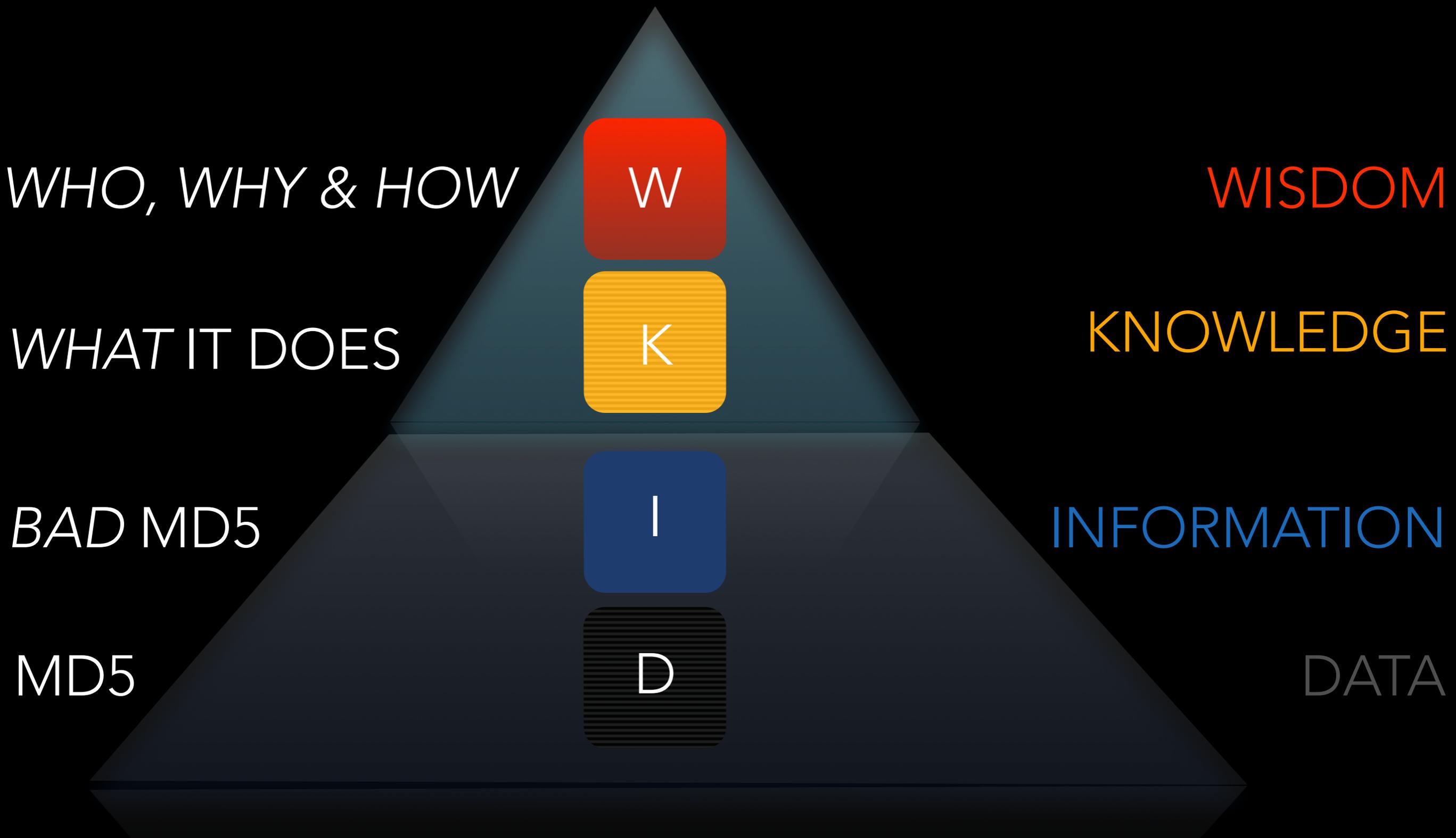
Over 2 Million Hits on Google....

CYBER THREAT INTELLIGENCE

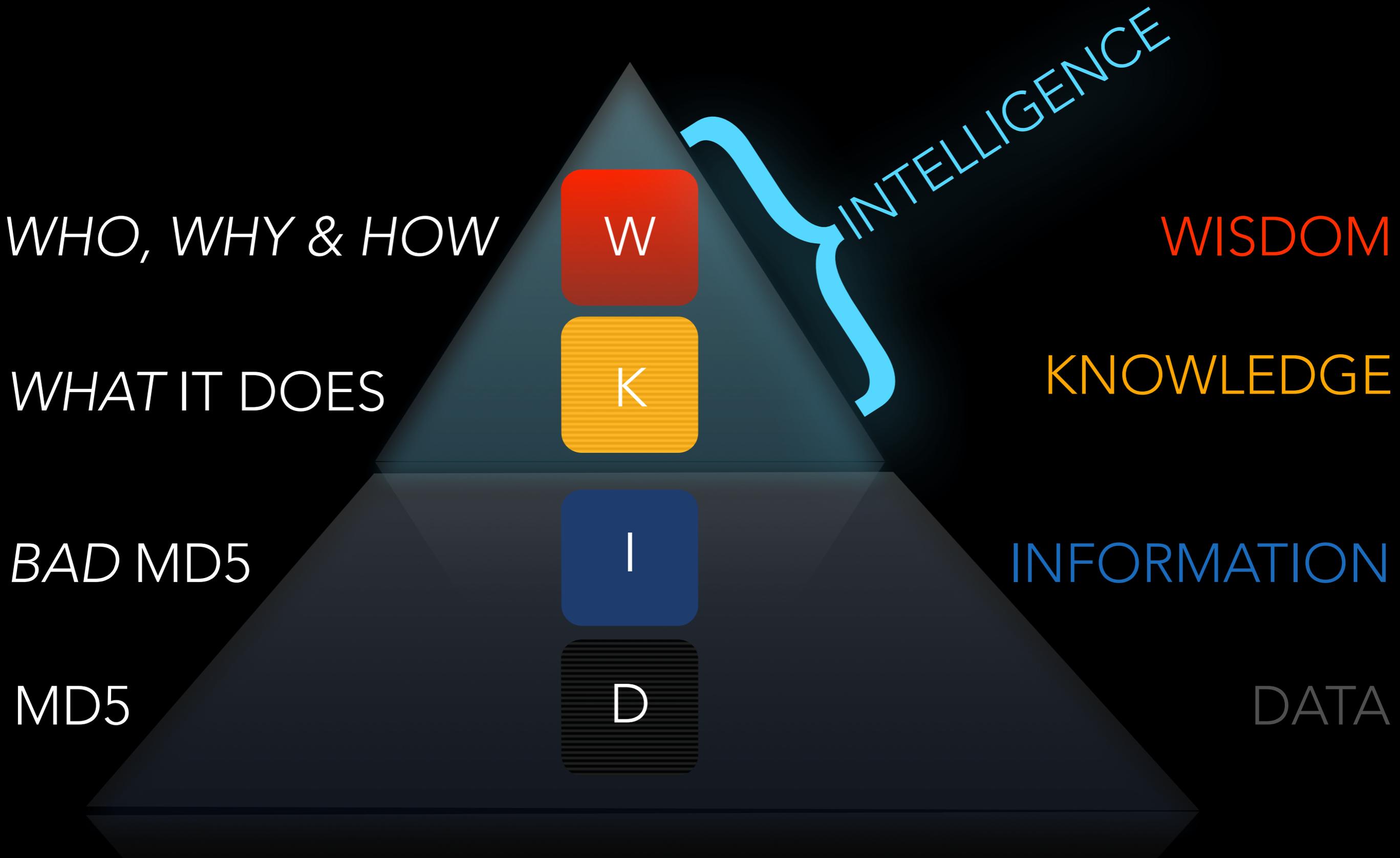


Over 2 Million Hits on Google....

WE CAN TURN TO INFORMATION
SCIENCE TO ILLUSTRATE THIS



WE CAN TURN TO INFORMATION
SCIENCE TO ILLUSTRATE THIS







W

GHOSTRAT EXAMPLE

W

Used by 14 different APT's targeting Hi-Tech IP, using these TTP's based on human analysis

K

Associated malware is a RAT with Y features

I

Bad because malware connected to it

D

103.20.192.xxx

GHOSTRAT C&C INFORMATION



1.QQQQ1234.PBZ, 1800-FRNEPU.PBZ, 1MNOFYJIA538A4V5GPWY.PBZ, 2001:PS8:1:12N1:0:QQQQ:8R66:P2Q6, 2001:PS8:1:N6R:0:QQQQ:5387:3SSS, 2005-FRNEPU.PBZ, 2X90.PA, 53000.UNAYBBI.PBZ, 54UGFS.PBZ, 8505.OKMIFRE.PBZ, 8505KK.OKMIFRE.PBZ, 8506.TNZRLXX.PBZ, 8506P.OKMIFRE.PBZ, 8510OK.OKMIFRE.PBZ, N.DVUVUHVUFURAT.ARG, NNPUEVFGZNF.PBZ, NPV.TENGVK.PBZ.OE, NPGVIRCEBGRPG.PA, NQNQVS.PBZ, NQYEKL.PBZ, NQJ.TERRA24.PB.XE, NWNVY.EH, NWXGXX.PBZ, NYPHDWSY.VF-N-YVORENY.PBZ, NYY.DGK333.PA, NAG.GERAM.CY, NBPRNP.PBZ, NEENLFNJ.PBZ, NFQ13.ARG, NIJNI.PBZ, NMYSFH.PBZ, O.NN1O2.PBZ, O.PBHTUFGHSSF.PBZ, O.F102-PAMM.PBZ, O8503O.UNAYBBI.PBZ, ONFRFEI.ARG, ORFGSERRQAF.VA, OTS45.BVPC.ARG, OYBT.FVAN.PBZ.PA, OHOOYRSRRO.ARG, OHFVARFF.ZVZBFNYNYN.PBZ, PVAGULNHCQNGRFREIRE.PBZ, PBZOVARYBG.PA, PBER2634.ENPVAT-JGS.PBZ, PBHAG.XRL5188.PBZ, Q.OAXFJ.PBZ, Q.JVKJJ.PBZ, Q1.SFSR9.PBZ, Q8502Q.UNAYBBI.PBZ, QNZAQFXW.PBZ, QRXF.BCYVCFVRF.PBZ, QVERPGXRLJBEQ.PB.XE, QBJA.QBJA-YBNO.PB.XE, QBJA.YYFTVAT.PBZ, QBJA003.SRAT6.HF, RSJPDY.PBZ, RVQBOV.PBZ, RBXHKM.PBZ, RCKZWF.PBZ, RKR.KVAAVNAXY.PBZ, S.JHP8.PBZ, S1-VASB.PM, SVJMI.ARG, SZBZ.WHNAQL.PBZ, SZBZ.CHOYVPIZ.PBZ, SBETBBTYRBAYL.PA, TRG38WJ262N.PBZ, TRJNMV.PBZ, TUB37.TUBFG-SVYR1.PBZ, TUB38.TUBFG-SVYR1.PBZ, TUBFGFRPGVBA.PBZ, TBYQNERN.OVM, U.JHP8.PBZ, UU.GBZB33.PBZ, UFURINY.PBZ, VTVLCH.PBZ, VZNTRF-ONFR.PBZ, VASB.958167.PBZ, VASHYVMVAT.PA, VBNMMB.PBZ, VCNEVATFNRYR.PBZ, WBXMNB.PBZ, XRUH1.UNATNZRCNL.PBZ, XRUH2.UNATNZRCNL.PBZ, XRUH3.UNATNZRCNL.PBZ, XRUH4.UNATNZRCNL.PBZ, XRLJBEQCBC.PBZ, XYVEBX.ARG, XBCHAN.PBZ, XBDLHLBQ.PA, XHXHGEHFGARG777.VASB, YVIRSVAQ1OYBTTVAT.PBZ, YY.QNHZAV.PBZ, ZRRYVGV.PBZ, ZRYGRKG.JBJVC.XE, ZVKZRQVNOVERPG.PA, ZWZBRV.PBZ, ZEXEKQ.PBZ, ZFFLFGRZ.VASB, ZKCMSQ.PBZ, ZLS2LBH.PBZ, ARJFBSS.ARG, AS.BHGREVASB.PBZ, AS82ZS-OSWWDLET61.PA, BANZRF0603.PBZ, BAYVARFCLJNERFPNAARE.ARG, BBI.YRENREN.PBZ, CNXFHFVP.PA, CPTAQT.PBZ, CBETNPVT.PA, CHWINP.PBZ, CHFFLGBVC.JF, CMEX.EH, DFPQSQQN.PA, DHNEGREGVA.VASB, DLTHZD.PBZ, EVSANFNK.PA, ECJBNX.PBZ, EFHC5.EVFBVAT.PBZ.PA, EFHC6.EVFBVAT.PBZ.PA, EILHWO.PBZ, F76M.PA, FNYBBATVAF.PA, FRNEPU-OHL.OVM, FREIREHCQNGRFBGJNER.PBZ, FVDVNB.TAJNL.ARG, FZNEG-VASB.PB.XE, FBCDLR.PBZ, FBF.FBBBBBBB.PBZ, FCNRVBRE.PBZ, FFF.969222.PBZ, GNAH.VASB, GNGENPXRE.ARG, GRFGNIEQBJA.PBZ, GUR.ZVPEBTBBQ.ARG, GVMVA.PA, GBRULN.PBZ, GBENATPBZM.PBZ, GENSSVPFGNGVP.PBZ, GELVGURER.ARG, GHPLRB.PBZ, GKG.TGULG.PBZ, GKG.XKJJV.PBZ, H1.TTBI88.PBZ, H3.PAPM.HF, H3.TTBBII.PBZ, H4.RFRG.PBZ.PA, H5.RFRG.PBZ.PA, HQRLCL.PBZ, HRTHFG.PBZ, HYGZVNERFBHEPRF.PBZ, HCQNGRFZ.PBZ, HCEGEVUFURFG.PBZ, IZVORB.PBZ, IZEGZB.PBZ, IBN.NOHCQNGR.XE, III.123FXL.OVM, IIKJ.ARG, J1.VVBB4567.PBZ, J18.IT, JO.FUVWVRQVLV.ARG, JVATFRNEPU.PB.XE, JVERQK.VA, JBBPNFVAB.PBZ, JGBCPBZCNAL.EH, JJJ.09FBH.PBZ, JJJ.5858JB.PBZ, JJJ.9651.ARG.PA, JJJ.OO-ORNGEVPR.PBZ, JJJ.POF.PB.XE, JJJ.QUSMQPYX.PBZ, JJJ.QWQWQNH.N.PBZ, JJJ.QBJAYBNO.JVAQBJFHCQNGR.PBZ, JJJ.RPBYR-FNVAG-FVZBA.ARG, JJJ.RQEBLK.EH, JJJ.SWMZAKSQ.PBZ, JJJ.TNZXESHX.PBZ, JJJ.TPZAFVIX.PBZ, JJJ.TRA365.PB.XE, JJJ.TZNFHBXEGN.PBZ, JJJ.UNCCLYBGHFYN.PBZ, JJJ.VASB-FREIVPR.PB.XE, JJJ.XWJER9SDJVRVYHBV.VASB, JJJ.XBOBNA.PBZ, JJJ.XBATMVCNGMV.PBZ, JJJ.XBGTNZGBN.PBZ, JJJ.XEBTNZRGB.PBZ, JJJ.YNSLREV.PBZ, JJJ.YRQLNMVYVZ.PBZ, JJJ.YRRFBHY.PB.XE, JJJ.YRTNYOVYTVFNLNE.PBZ, JJJ.YBIRLBHFUVCA.PBZ, JJJ.ZVENYVIR.PA, JJJ.ZYPPK.PBZ, JJJ.ZBHFRRERYRNF.R.PBZ, JJJ.ZLOEBVYRE.PBZ, JJJ.DVADVAKVNGVNB.PBZ, JJJ.FPRAGXBERN.PBZ, JJJ.FBLHXGNZO.PBZ, JJJ.FEFE.PB.XE, JJJ.FLNGGHF.PBZ.OE, JJJ.GNAQSHLXB.PBZ, JJJ.GBCNAV.PBZ, JJJ.GLJWW.PBZ, JJJ.I3YVGR.PBZ, JJJ.JBCKF.PBZ, JJJ.MUBHZBLATBZ.PBZ, JJJ9.JVXVCYHZ.PBZ, JLLHJI.PBZ, JM1.275CX.PBZ, JM4.275CX.PBZ, KVN.DVUVUHVUFURAT.ARG, KVA.KVAAVNAXY.PBZ, KVA8QN.PBZ, KXJFYJ.PBZ, KKK.ONB01.PBZ, LXMPWIOS.VGRZQO.PBZ, LBHNFXRQURQBZNV.A.PA, LDGKIFY.PBZ, LEGDUE.PBZ, LHPRYPNIQNE.PBZ, LIHGLD.PBZ, MNAMBHY.NLN.PBZ.FL, MVSPIZ.PBZ, MLCCVN.PBZ

GH0STRAT KNOWLEDGE



K

TAKE FULL CONTROL OF THE REMOTE SCREEN ON THE INFECTED BOT
PROVIDE REAL TIME AS WELL AS OFFLINE KEYSTROKE LOGGING
PROVIDE LIVE FEED OF WEBCAM, MICROPHONE OF INFECTED HOST
DOWNLOAD REMOTE BINARIES ON THE INFECTED REMOTE HOST
TAKE CONTROL OF REMOTE SHUTDOWN AND REBOOT OF HOST
DISABLE INFECTED COMPUTER REMOTE POINTER AND KEYBOARD INPUT
ENTER INTO SHELL OF REMOTE INFECTED HOST WITH FULL CONTROL
PROVIDE A LIST OF ALL THE ACTIVE PROCESSES
ETC.

GH0STRAT WISDOM

W

THE ABILITY TO LINK THREE DISTINCT CAMPAIGNS TO THE SAME THREAT ACTORS BY ANALYZING ATTACK C&C INFRASTRUCTURE, COMPILE TIMES, RESOLVED IP'S, A SIMILAR XOR'D ZXHELL PAYLOAD, ZERO-DAY FLASH EXPLOITS, WATERING HOLE VECTOR, ATTACK MOVEMENT TTP'S DURING IR, AND MORE

THE ABILITY TO WARN OTHERS IN THE SAME TARGETED SECTORS OF THIS WATERING HOLE STYLE ATTACK, AND THE RELATED TTP'S OF THE THREAT ACTORS TO IMPROVE BOTH DETECTION AND RESPONSES WITHIN THE SECTOR

THE ABILITY TO MAKE SIMILAR ATTACKS MORE EXPENSIVE BY SENDING UNIQUE HIGH QUALITY IOCS TO EVERY CUSTOMER AROUND THE WORLD SUCH THAT RE-USING EITHER PORTIONS OF CODE AND/OR DIFFERENT TTP'S ONCE INSIDE, BECOMES MUCH HIGHER RISK FOR THE ATTACKER

THE ABILITY TO WORK WITH MICROSOFT IMMEDIATELY ON A PATCH FOR THE RELATED IE ZERO-DAY BEING USED AND LEVERAGE THEIR ABILITY TO PUSH A WORLDWIDE PATCH QUICKLY

GHOSTRAT WISDOM

Ephemeral
Hydra

public sector: defence, law, IT and mining

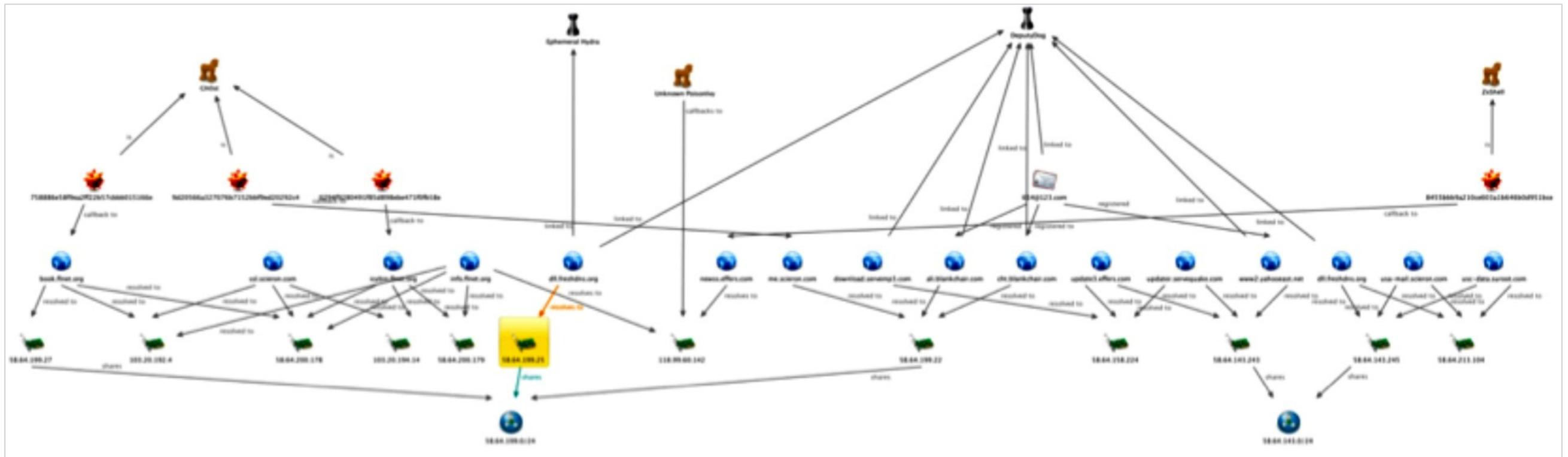
Operation
SnowMan

US military veterans website VFW.org

APT 17

Deputy
Dog

public sector: defence, law, IT and mining



THE ABILITY TO LINK THREE DISTINCT CAMPAIGNS TO THE SAME THREAT ACTORS BY ANALYZING ATTACK C&C INFRASTRUCTURE, COMPILE TIMES, RESOLVED IP'S, A SIMILAR XOR'D ZXHELL PAYLOAD, ZERO-DAY FLASH EXPLOITS, WATERING HOLE VECTOR, ATTACK MOVEMENT TTP'S DURING IR, AND MORE

JUST A FEW WORDS ON PERSISTENCE
AND THE HUMAN...

HOW THEY USED TO STAY PERSISTENT ON THE HOST

Autoexec.bat:

```
@ECHO OFF
SET SOUND=C:\PROGRA~1\CREATIVE\CTSND
SET BLASTER=A220 I5 D1 H5 P330 E620 T6
SET PATH=C:\WINDOWS;C:\
LH C:\WINDOWS\COMMAND\MSCDEX.EXE /D:123
C:\DOS\MYMALWARE.EXE /X
```

Batch File to Clean Up After (delete MYMALWARE.EXE):

```
@ECHO OFF
D
DEL "C:\DOS\MYMALWARE.EXE"
IF EXIST "C:\USERS\LAB\DESKTOP\MYMALWARE.EXE" GOTO D
DEL /F "C:\USERS\LAB\APPDATA\LOCAL\TEMP\CLEANERBAT.BAT"
```

HOW THEY STAY PERSISTENT NOW...

SideBar Gadgets
Backdooring DLL's
DLL Load Order Manipulation
Shortcut HiJacking
File Association HiJack
Windows Application Compatibility
Bootkits
Master Boot Record
Volume Boot Recored
BIOS/UEFI Malware
HypberVisor/Ring1 Rootkit
System Management Mode
Intel® Active Management Technology root kit
Add SUPPORT User Account with a 500 RID
Malicious Firmware Update
Hidden Boot Devcies
Network Boot level backdoors
Software Vulnerabilities

Internet Explorer / Browser Helper Objects
Explorer.exe
Logon Registry Entries
Codecs
Boot Execute
Image HiJacks / Sticky Keys
Applnt
Known DLLs
WinLogon
Winsock Providers
Print Monitors
LSA Providers
Network Providers
WMI Filters
Schedule Tasks
Services
Drivers

HOW THEY STAY PERSISTENT NOW...

- SideBar Gadgets
- Backdooring DLL's
- DLL Load Order Manipulation
- Shortcut HiJacking
- File Association HiJack
- Windows Application Compatibility
- Bootkits
 - Master Boot Record
 - Volume Boot Recored
 - BIOS/UEFI Malware
 - HypberVisor/Ring1 Rootkit
 - System Management Mode
- Intel® Active Management Technology root kit
- Add SUPPORT User Account with a 500 RID
- Malicious Firmware Update
- Hidden Boot Devcies
- Network Boot level backdoors
- Software Vulnerabilities

- Internet Explorer / Browser Helper Objects 13
 - Explorer.exe 71
 - Logon Registry Entries 42
 - Codecs
 - Boot Execute 5
- Image HiJacks / Sticky Keys 13
 - Applnt 3
 - Known DLLs 1
 - WinLogon 7
- Winsock Providers 4
- Print Monitors 1
- LSA Providers 5
- Network Providers
- WMI Filters
- Schedule Tasks
- Services
- Drivers

HOW THEY USED TO STAY PERSISTENT ON THE DOMAIN

Add domain user and put them in Domain Admins group

```
NET USER USERNAME PASSWORD /ADD /DOMAIN  
NET GROUP "DOMAIN ADMINS" USERNAME /ADD /DOMAIN
```

Add local user and put them Local Administrators group

```
NET USER USERNAME PASSWORD /ADD  
NET LOCALGROUP ADMINISTRATORS USERNAME /ADD
```

HOW THEY DO IT NOW

Use Group Policy to backdoor Servers/
Workstations

Backdoor patch management tools

Weaken AD policies (e.g. re-enable
NTLM)

Steal Windows Root / CA keys

Uninstall Security Patches

Modify Proxy PAC file, allow IP, force
auth, grab hashes

Malicious Symlinks to shares to collect
SMB hashes

Custom NTP for DC's to mod
timestamps

Grant VPN rights to accounts

Logon Scripts

Create new admin user or elevate user
and reset PW

Dump hashes for cracking or pass-the-
hash

Backdoor the laptop Admin logs in
from - Roaming Profile

Backdoor a DC server

Backdoor Files on Net Shares that
Admins Use

Changing Ownership/Permissions on
AD Partitions

Mimikatz AddSID (Hide Admin Privs
with SID history)

Golden Tickets

Silver Tickets

PowerShell!

CASE STUDY: CLANDESTINE FOX



CASE STUDY: CLANDESTINE FOX

MARCH, 2013

NEW TARGET(S): 01

NEW VICTIM(S): 01

INTELLIGENCE: THREAT ACTOR TTP



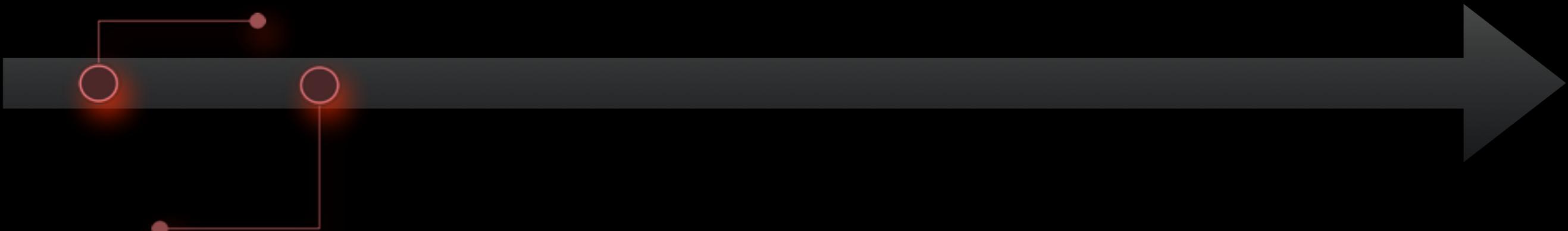
CASE STUDY: CLANDESTINE FOX

MARCH, 2013

NEW TARGET(S): 01

NEW VICTIM(S): 01

INTELLIGENCE: THREAT ACTOR TTP



APRIL 25, 2014

TARGET(S): 01

NEW VICTIM(S): 01

INTELLIGENCE: POTENTIAL 0-DAY

CASE STUDY: CLANDESTINE FOX

MARCH, 2013

NEW TARGET(S): 01

NEW VICTIM(S): 01

INTELLIGENCE: THREAT ACTOR TTP



APRIL 25, 2014

TARGET(S): 01

NEW VICTIM(S): 01

INTELLIGENCE: POTENTIAL 0-DAY

TARGET(S): 02

NEW VICTIM(S): 00

INTELLIGENCE: IP & DOMAIN IOCS,
COORDINATED BLOG WITH
MICROSOFT ON 0-DAY, ID:APT3

CASE STUDY: CLANDESTINE FOX

MARCH, 2013

NEW TARGET(S): 01

NEW VICTIM(S): 01

INTELLIGENCE: THREAT ACTOR TTP

TARGET(S): 02

NEW VICTIM(S): 00

INTELLIGENCE: NETWORK & ENDPOINT
MUTEX BASED IOC

APRIL 25, 2014

TARGET(S): 01

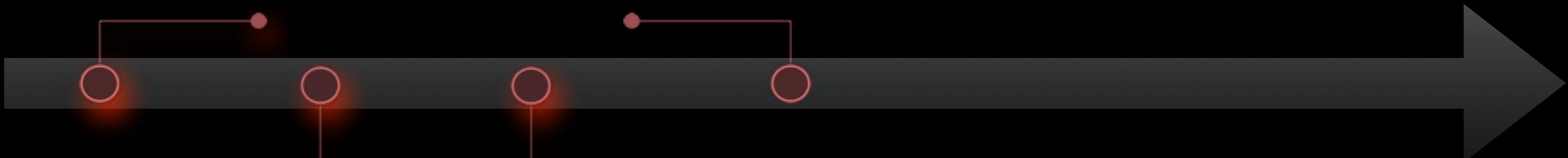
NEW VICTIM(S): 01

INTELLIGENCE: POTENTIAL 0-DAY

TARGET(S): 02

NEW VICTIM(S): 00

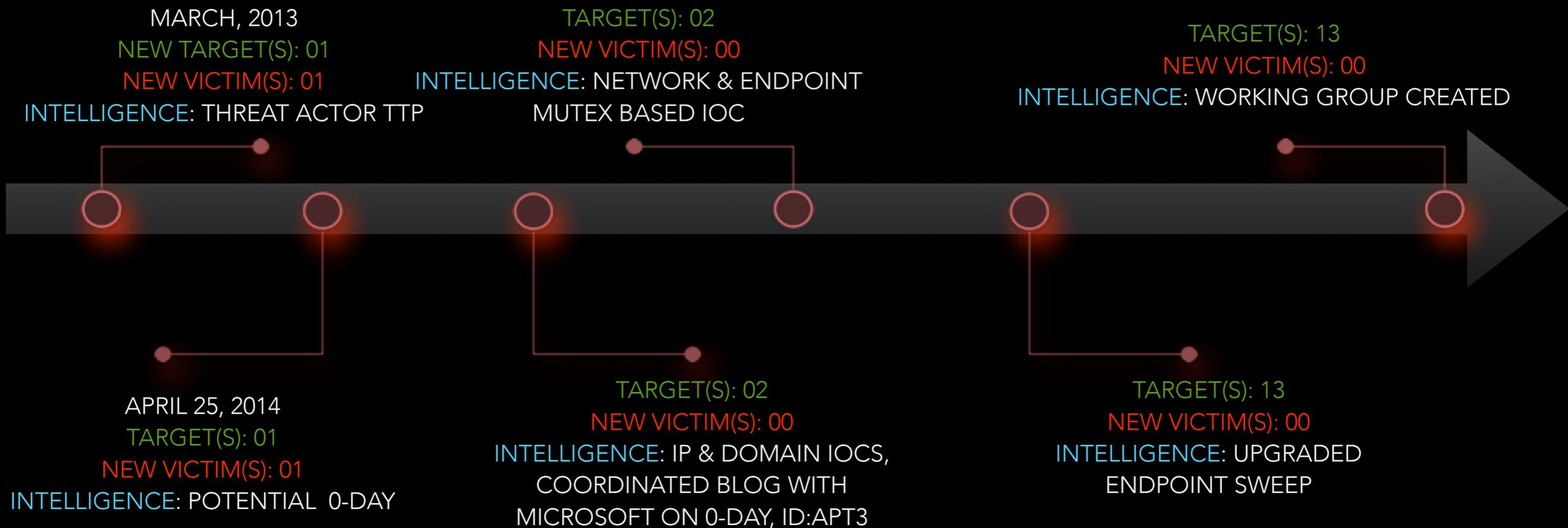
INTELLIGENCE: IP & DOMAIN IOCS,
COORDINATED BLOG WITH
MICROSOFT ON 0-DAY, ID:APT3



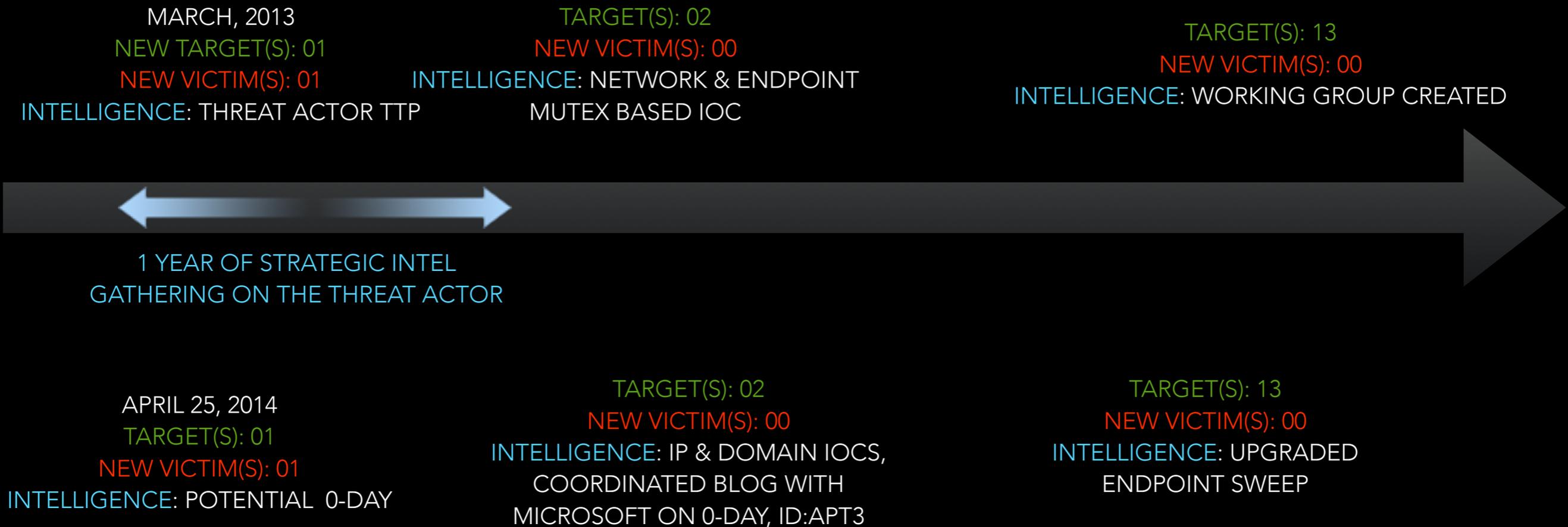
CASE STUDY: CLANDESTINE FOX



CASE STUDY: CLANDESTINE FOX



CASE STUDY: CLANDESTINE FOX



CASE STUDY: CLANDESTINE FOX



CASE STUDY: CLANDESTINE FOX



SAME EXPLOIT ATTEMPTED AT 13 CUSTOMER SITES
ATTACKER SUCCESS RATE: 0%

SO WE SEE THERE IS A FUNDAMENTAL
DIFFERENCE BETWEEN INFORMATION
AND *INTELLIGENCE*

Information vs. Intelligence

INFORMATION	INTELLIGENCE
RAW, UNFILTERED DATA	PROCESSED, SORTED, AND DISTILLED INFORMATION
UNEVALUATED WHEN DELIVERED	EVALUATED AND INTERPRETED BY TRAINED EXPERT ANALYSTS
AGGREGATED FROM VIRTUALLY EVERY SOURCE	AGGREGATED FROM RELIABLE SOURCES AND CROSS CORRELATED FOR ACCURACY
MAY BE TRUE, FALSE, MISLEADING, INCOMPLETE, RELEVANT, OR IRRELEVANT	ACCURATE, TIMELY, COMPLETE ASSESSED FOR RELEVANCY

Information vs. Intelligence

INFORMATION	INTELLIGENCE
RAW, UNFILTERED DATA	PROCESSED, SORTED, AND DISTILLED INFORMATION
UNEVALUATED WHEN DELIVERED	EVALUATED AND INTERPRETED BY TRAINED EXPERT ANALYSTS
AGGREGATED FROM VIRTUALLY EVERY SOURCE	AGGREGATED FROM RELIABLE SOURCES AND CROSS CORRELATED FOR ACCURACY
MAY BE TRUE, FALSE, MISLEADING, INCOMPLETE, RELEVANT, OR IRRELEVANT	ACCURATE, TIMELY, COMPLETE ASSESSED FOR RELEVANCY

K

W

W

W

SO WHAT WOULD *WISDOM* TELL
US THE NEW PARADIGM IS THEN?

SO WHAT WOULD *WISDOM* TELL
US THE NEW PARADIGM IS THEN?

SPOILER ALERT: IT'S UGLY!

THE NEW PARADIGM, ASSUMPTIONS

- ATTACKER HAS YOUR DOMAIN ADMIN PRIVILEGES
- ATTACKER HAS HASHES OR CRACKED PASSWORDS FOR ALL YOUR DOMAIN ACCOUNTS
- ATTACKER CAN FREELY MOVE VIA VPN'S AND HOST TO HOST
- YOUR PARTNER NETWORKS MAY BE COMPROMISED
- CRIMEWARE AND APT TTP's ARE CONVERGING



THE NEW PARADIGM, ASSUMPTIONS

- ATTACKER HAS YOUR DOMAIN ADMIN PRIVILEGES
- ATTACKER HAS HASHES OR CRACKED PASSWORDS FOR ALL YOUR DOMAIN ACCOUNTS
- ATTACKER CAN FREELY MOVE VIA VPN'S AND HOST TO HOST
- YOUR PARTNER NETWORKS MAY BE COMPROMISED
- CRIMEWARE AND APT TTP's ARE CONVERGING



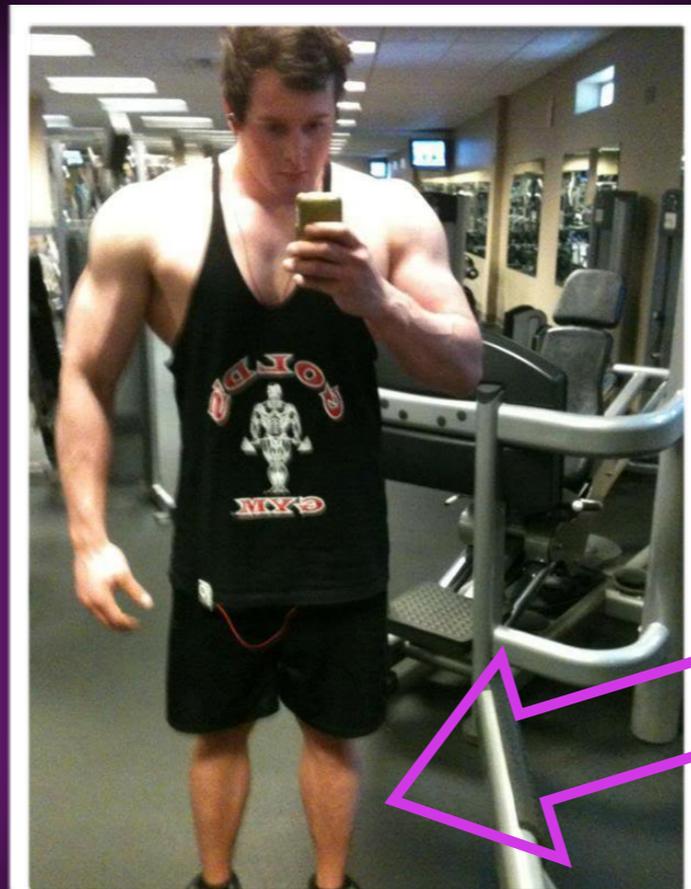
THE NEW PARADIGM, WEAKNESSES

- YOU CAN'T DETECT SIGNATURE-LESS SPEAR PHISHING ATTACKS
- YOU HAVE POOR CREDENTIAL MANAGEMENT
- YOUR NETWORKS ARE NOT EFFECTIVELY SEGREGATED
- YOU ARE STILL USING SINGLE FACTOR AUTH FOR VPN / OWA
- YOUR SECURITY SAFEGUARDS ARE NOT ARMED FROM PRIVILEGED ACCOUNTS
- YOU ARE NOT YET COLLECTING DATA THAT IS CRITICAL DURING INCIDENT RESPONSE



THE NEW PARADIGM, WEAKNESSES

- YOU CAN'T DETECT SIGNATURE-LESS SPEAR PHISHING ATTACKS
- YOU HAVE POOR CREDENTIAL MANAGEMENT
- YOUR NETWORKS ARE NOT EFFECTIVELY SEGREGATED
- YOU ARE STILL USING SINGLE FACTOR AUTH FOR VPN / OWA
- YOUR SECURITY SAFEGUARDS ARE NOT ARMED FROM PRIVILEGED ACCOUNTS
- YOU ARE NOT YET COLLECTING DATA THAT IS CRITICAL DURING INCIDENT RESPONSE



weak!

THE NEW PARADIGM, CAPABILITIES

- Intelligence, not information (rich context alerts, information on who, not what)
- Fast path to perimeter update (from unknown to known, local to your network)
- Fast pivot to IR with Rapid Response Capability (hint: retainer services are your friend)
- Constant hunting... how much? Answer: How bad do you care about persistence?



THE NEW PARADIGM, BATTLEFIELD

- Make attacks more expensive and higher risk
- Become more offensive in your defense
- Make the attacker *feel you*, no matter what they do, where they go
- Trick the attacker, Poke the attacker, Annoy the attacker, **Expose the attacker**
- Play Man-to-Man defense —> follow, stay tight, *change* the narrative/outcome!
- Attack *their* supply chain, poison markets
- Re-Imagine the game, entirely, every day



THE NEW PARADIGM, BATTLEFIELD

- Make attacks more expensive and higher risk
- Become more offensive in your defense
- Make the attacker *feel you*, no matter what they do, where they go
- Trick the attacker, Poke the attacker, Annoy the attacker, **Expose the attacker**
- Play Man-to-Man defense —> follow, stay tight, *change the narrative/outcome!*
- Attack *their* supply chain, poison markets
- Re-Imagine the game, entirely, every day

APT 17

Microsoft®
TechNet



THE NEW PARADIGM, THE FUTURE

- More destructive attacks
- Attribution becomes more important
- Counter-forensics will get really, really good. Like, really.
- Attacks will align with conflicts, every time
- More government involvement in both defense and offense
- Cyber bounty-hunting, rewards, wanted posters on the 'net
- Cyber-Darwinism will level the playing field out of sheer necessity (survivalism)
- No more moral high ground restraint. The right to defend and fire weapons on intruders.
- CYBER LAWYERZ GONE WILD! (and the need to indemnify the protectors and victims from liability... **SMART ACT!**)



THE NEW PARADIGM, THE FUTURE

- More destructive attacks
- Attribution becomes more important
- Counter-forensics will get really, really good. Like, really.
- Attacks will align with conflicts, every time
- More government involvement in both defense and offense
- Cyber bounty-hunting, rewards, wanted posters on the 'net
- Cyber-Darwinism will level the playing field out of sheer necessity (survivalism)
- No more moral high ground restraint. The right to defend and fire weapons on intruders.
- CYBER LAWYERZ GONE WILD! (and the need to indemnify the protectors and victims from liability... **SMART ACT!**)



TWO LEVELS OF SAFETY PROTECTION CAN BE AWARDED



Government Contractor Defense

**CERTIFIED
(HIGH CONFIDENCE OF CONTINUED EFFECTIVENESS)**



Only a Liability Cap

**FULL DESIGNATION
(PROVEN EFFECTIVE)**

OR

**DEVELOPMENTAL TEST AND EVAL
(SHOWS PROMISE, NEEDS WORK)**

DT&E
Designation

TWO LEVELS OF SAFETY PROTECTION CAN BE AWARDED



Government Contractor Defense

**CERTIFIED
(HIGH CONFIDENCE OF **CONTINUED** EFFECTIVENESS)**



Only a Liability Cap

**FULL DESIGNATION
(PROVEN EFFECTIVE)**

OR

**DEVELOPMENTAL TEST AND EVAL
(SHOWS PROMISE, NEEDS WORK)**

DT&E
Designation

WHAT ARE SOME ITEMS DHS EXAMINED FOR US TO BECOME *CERTIFIED*?

EXTENSIVE OPERATIONAL ENVIRONMENT TESTING:

LOW FALSE POSITIVE AND FALSE NEGATIVE RATES

HIGH PROBABILITY OF DETECTION

CONSISTENT LONG-TERM RESULTS

CONFORMANCE TO OUR STATED SPECIFICATIONS

DOMAIN EXPERTISE WAS READILY AVAILABLE

APPLICABLE STANDARDS WERE MET

FAVORABLE CUSTOMER FEEDBACK

PERFORMANCE AS INTENDED

DOCUMENTED QA PLANS

PROVEN REPEATABILITY

PROVEN LOW MTBF



WHAT ARE SOME ITEMS DHS EXAMINED FOR US TO BECOME *CERTIFIED*?

EXTENSIVE OPERATIONAL ENVIRONMENT TESTING:

LOW FALSE POSITIVE AND FALSE NEGATIVE RATES

HIGH PROBABILITY OF DETECTION

CONSISTENT LONG-TERM RESULTS

CONFORMANCE TO OUR STATED SPECIFICATIONS

DOMAIN EXPERTISE WAS READILY AVAILABLE

APPLICABLE STANDARDS WERE MET

FAVORABLE CUSTOMER FEEDBACK

PERFORMANCE AS INTENDED

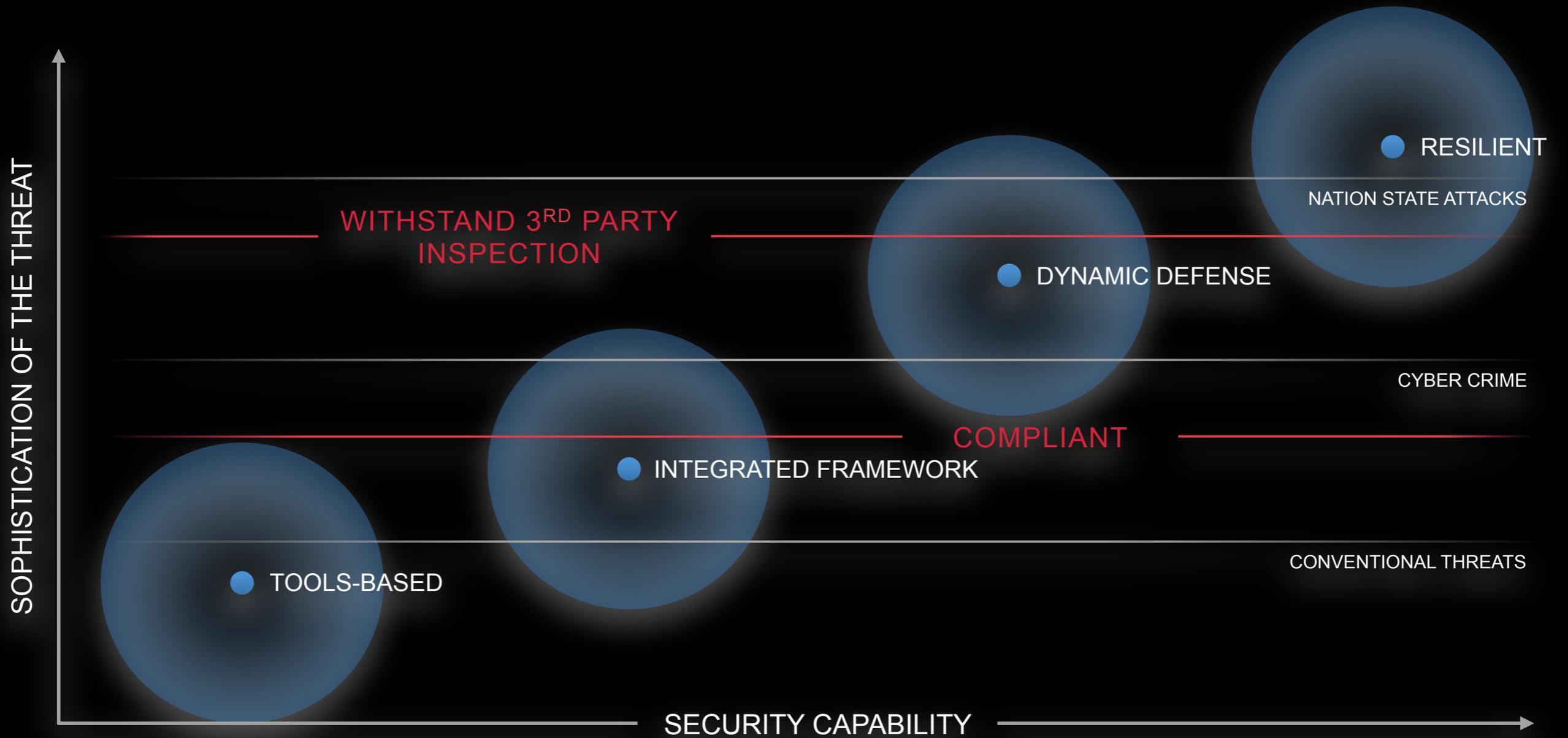
DOCUMENTED QA PLANS

PROVEN REPEATABILITY

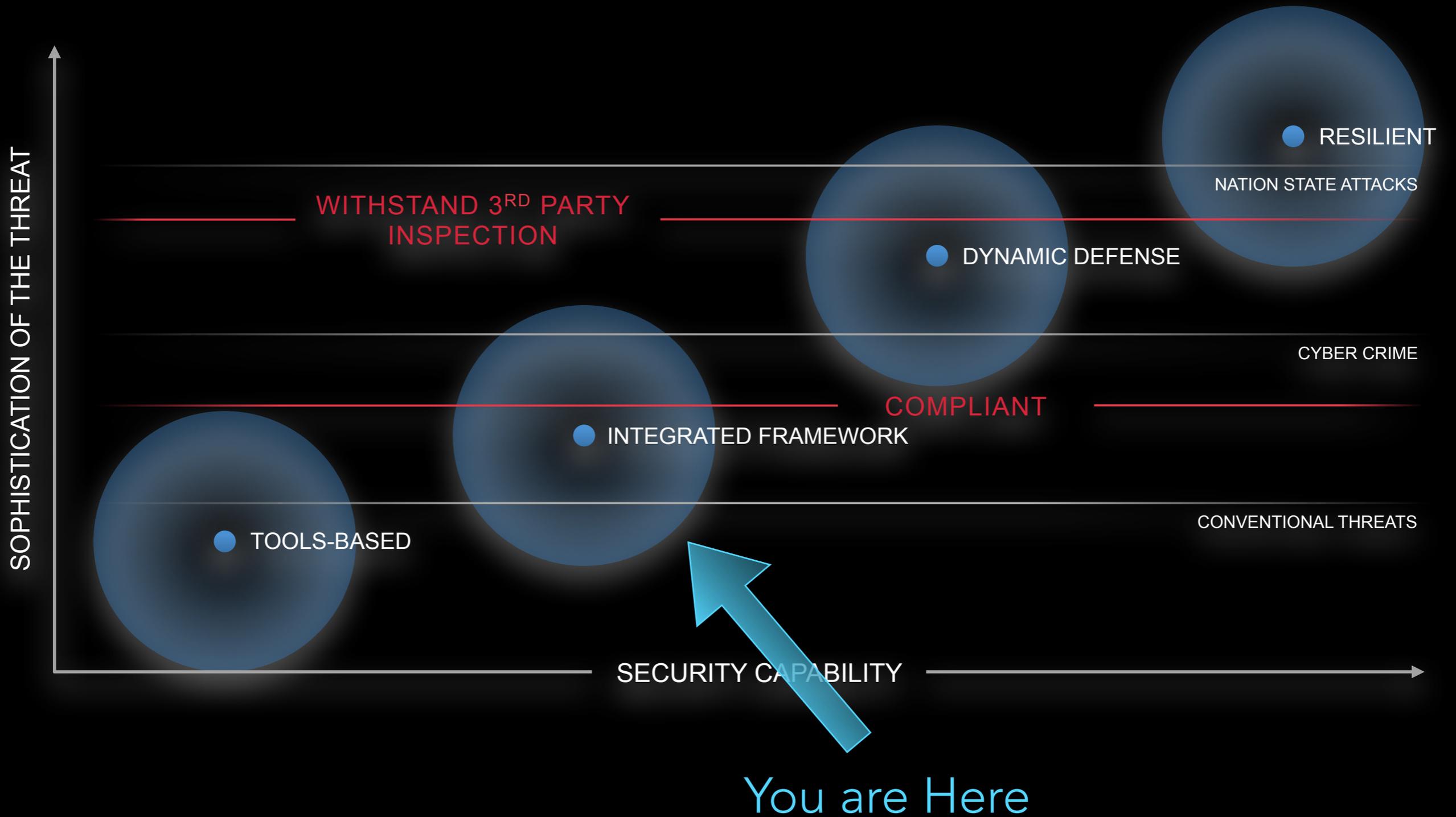
PROVEN LOW MTBF



THE NEW PARADIGM, MATURITY



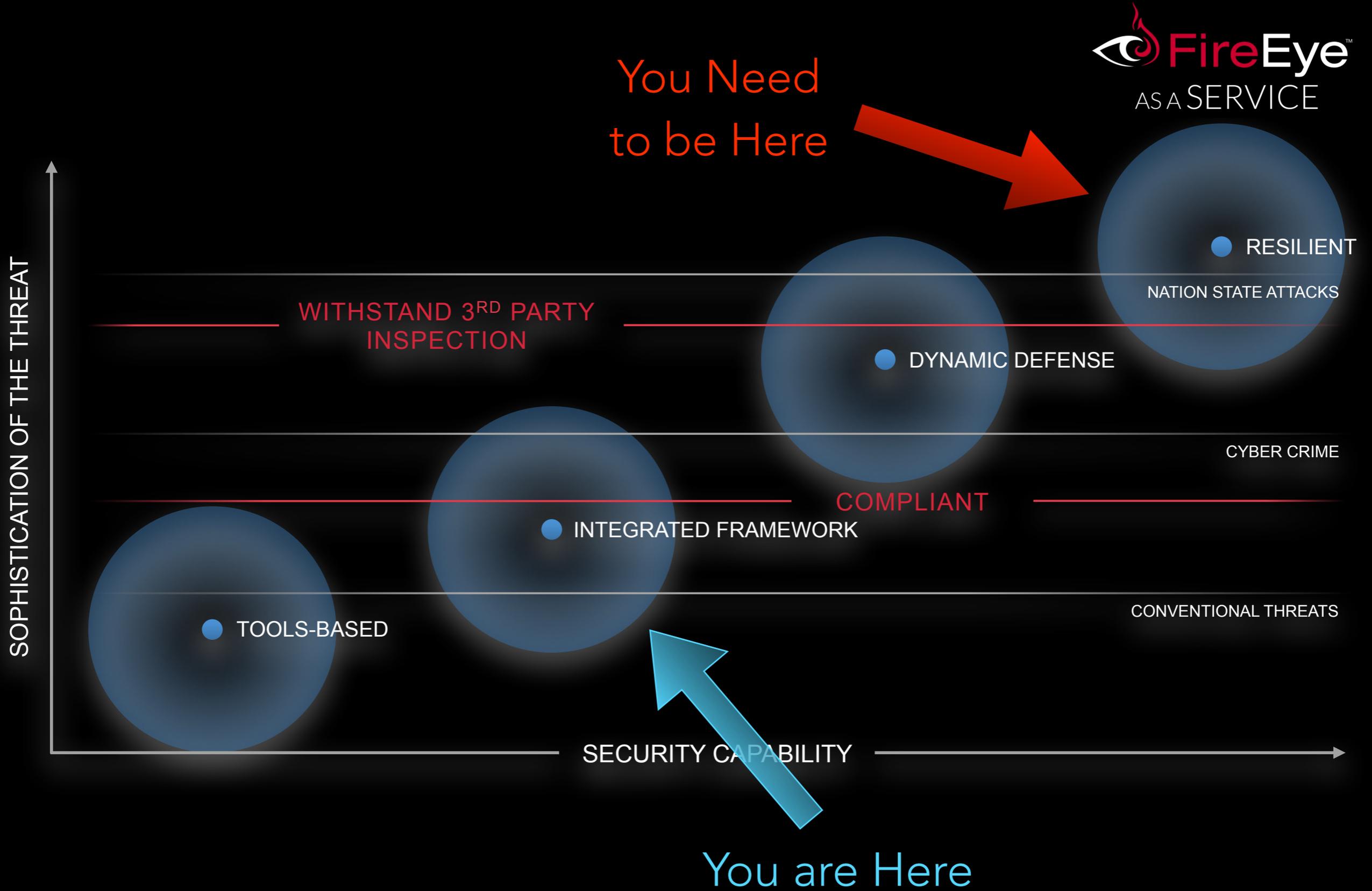
THE NEW PARADIGM, MATURITY



THE NEW PARADIGM, MATURITY



THE NEW PARADIGM, MATURITY



You Need to be Here

You are Here

TYPICAL DAY IN THE LIFE OF FAAS (ACTUAL MINING COMPANY CASE STUDY)

Clean up and Lean Forward Protection

Based on threat intelligence, FaaS not only helps cleanup the current threat but protect the customer for what might follow

00:45 Containment and Response Recommendation

Avoid the "whack-a-mole" approach and instead understand the threat actor while responding

Analysis

FaaS analysts and responders analyze the infected systems and callback channels; found total of 52 compromised machines

0:00 A Malicious Event

FireEye as a Service (FaaS) monitoring a customer site discovers a compromised system

0:05 Targeted Attack

FaaS analysts quickly discover 26 compromised systems

0:15 Customer Notification

FaaS recommendation: DO NOTHING!
... for now.



THE NEW PARADIGM, YOU

“The height of your accomplishments will equal the depth of your convictions.”

William F. Scolavino



QUESTIONS?



QUESTIONS?