BlackBerry | CYLANCE

Neutralizing Today's Cyber Threats

Fighting the Zombie Apocalypse

Sig Murphy
Senior Director of Professional Services

OUR MISSION

Our mission is to protect every computer, user and object under the sun.

Safe Harbor

The information in this presentation is confidential and proprietary to Cylance® and may not be disclosed without the permission of Cylance. This presentation is not subject to your license agreement or any other service or subscription agreement with Cylance. Cylance has no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein.

This document, or any related presentation and Cylance's strategy and possible future development, product, and/or platform direction and functionality are all subject to change and may be changed by Cylance at any time for any reason without notice. The information on this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. This document is for informational purposes and may not be incorporated into a contract. Cylance assumes no responsibility for errors or omissions in this document.

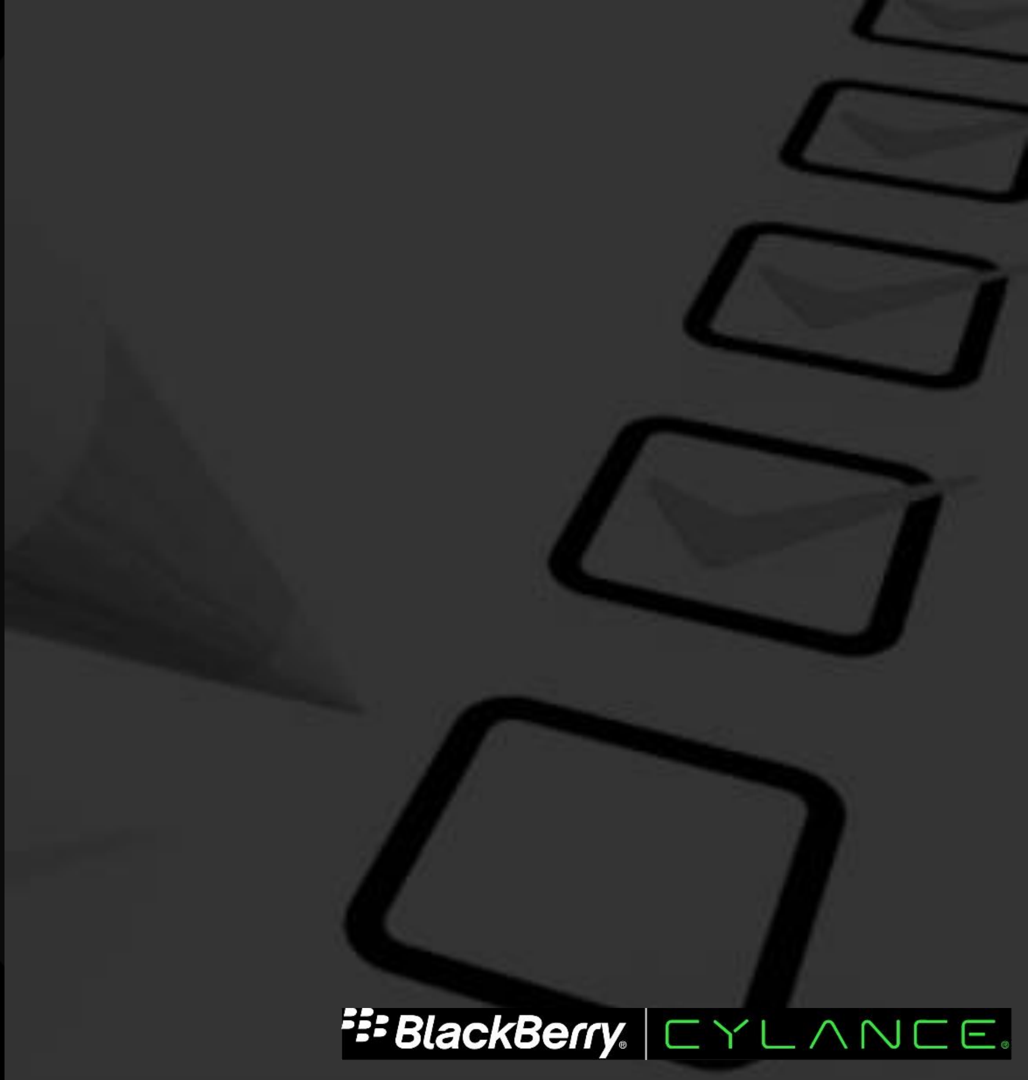
SIG MURPHY

- Formerly at Fidelis and the DoD Cybercrime Center (DC3; IA and CI)
- Husband, Father, Maker and Gamer (time allowing)
- Senior Director of Consulting Services for BlackBerry Cylance

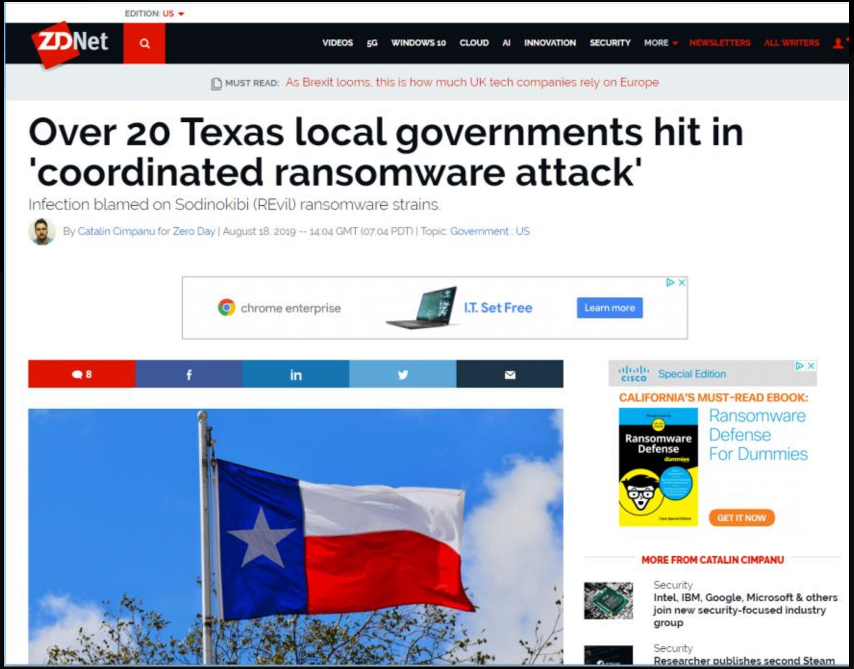
BlackBerry | CYLANCE

AGENDA

- Current Events
- The Evolution of Sodinokibi
- TrickBot or treat?
- Demo
- Evolving to Prevention
- Q & A



CURRENT EVENTS


EDITION: US
ZDNet
VIDEOS 5G WINDOWS 10 CLOUD AI INNOVATION SECURITY MORE NEWSLETTERS ALL WRITERS

MUST READ: As Brexit looms, this is how much UK tech companies rely on Europe

Over 20 Texas local governments hit in 'coordinated ransomware attack'

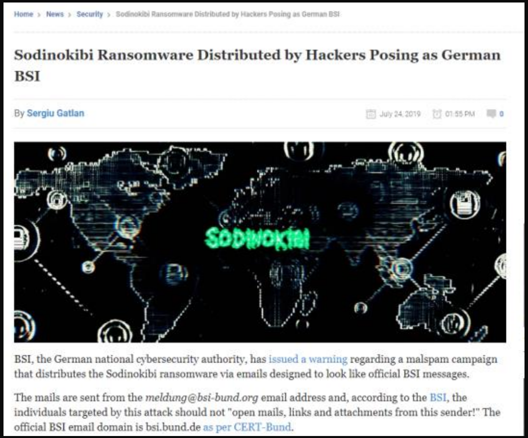
Infection blamed on Sodinokibi (REvil) ransomware strains.

By Catalin Cimpanu for Zero Day | August 18, 2019 -- 14:04 GMT (07:04 PDT) | Topic: Government : US

MORE FROM CATALIN CIMPANU

Security
Intel, IBM, Google, Microsoft & others join new security-focused industry group

Security
Researcher publishes second Steam

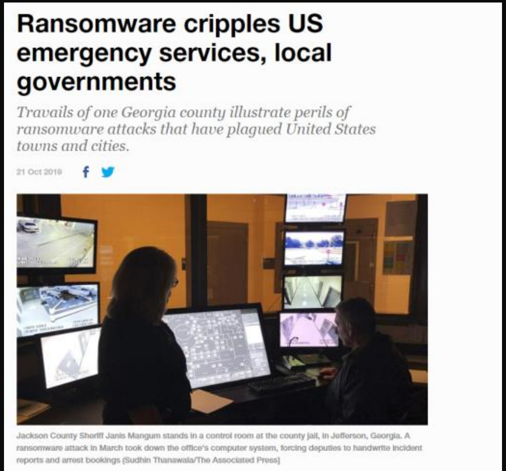

Home > News > Security > Sodinokibi Ransomware Distributed by Hackers Posing as German BSI
SODINOKIBI

Sodinokibi Ransomware Distributed by Hackers Posing as German BSI

By Sergiu Gatlan July 24, 2019 01:55 PM 0

BSI, the German national cybersecurity authority, has issued a warning regarding a malspam campaign that distributes the Sodinokibi ransomware via emails designed to look like official BSI messages.

The mails are sent from the *meldung@bsi-bund.org* email address and, according to the BSI, the individuals targeted by this attack should not "open mails, links and attachments from this sender!" The official BSI email domain is bsi.bund.de as per CERT-Bund.

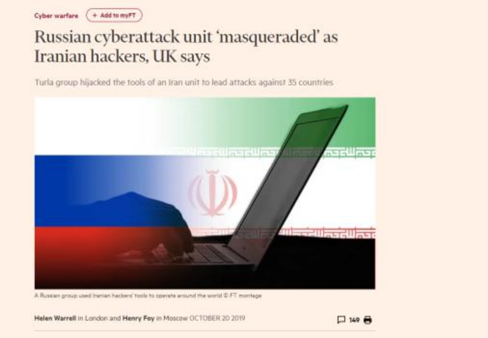


Ransomware cripples US emergency services, local governments

Travails of one Georgia county illustrate perils of ransomware attacks that have plagued United States towns and cities.

21 Oct 2019

Jackson County Sheriff Janis Mangum stands in a control room at the county jail, in Jefferson, Georgia. A ransomware attack in March took down the office's computer system, forcing deputies to handwrite incident reports and arrest bookings (Sudhin Thanawala/The Associated Press]



Russian cyberattack unit 'masqueraded' as Iranian hackers, UK says

Turla group hijacked the tools of an Iran unit to lead attacks against 35 countries

A Russian group used Iranian hackers' tools to operate around the world © FT montage

Helen Warrell in London and **Henry Foy** in Moscow OCTOBER 20 2019 149

EVOLUTION OF SODINOKIBI

WHAT ARE THESE VARIANTS?

Malware: GandCrab

Delivery: RAAS. Malvertizing, Spearphishing, Infected MSPs. Gandcrab terminates all locked processes, encrypts specific file extensions and presents a ransom note.

Impact: By May 2019, Gandcrab was responsible for over half of all new ransomware infections. Over “$2B” in ransom paid with “$150M” to the authors.

Malware: Sodnokibi

Delivery: RAAS. CVE-2019-2725, Malvertizing, RDP Drive-bys, Spearphishing, Infected MSPs. Sodnokibi terminates all locked processes, encrypts specific file extensions and presents a ransom note.

Impact: Fastest growing ransomware threat since Spring of 2019. Grants attackers Admin access via CVE-2018-8453.

TRICK(BOT) OR TREAT?

TRICKBOT EXPLAINED

Malware: Trickbot

- Features:
- Infection happens through weaponized Word and Excel documents from banks/services with embed macros. These drop downloader .bat files
- Malware is downloaded into the %APPDATA% \Roaming folder and executed
- Uses process hollowing to insert itself into svchost.exe
- Deletes many different antivirus (AV) software from system
- Creates scheduled tasks on the system for persistence
- Tests Internet connectivity
- Uses Transport Layer Security (TLS) to encrypt communications
- Once successful it connects to its C2 servers, pulls its various modules and updates
- Modules collect information off the system and browsing credentials, mostly focusing on online banking
- Malware attempts to spread across network to acquire further bots/victims using its various its worm modules

TAKING A STEP BACK

WE LIVE IN A WORLD OF EXTRAORDINARY CRIMES

Cyber c… the world $6 tril… up from $3 trillion in 2…

“The a… mber is now esti… year of … the greatest tra… th in history […] and is more profita… n the global trade … gs ($652B) and even all of counterfeiting ($1.13T) COMBINED

e… 2… es roughly $300… 2017 … lost to natural catastrophes

- John Drzik, President of Global Risk and Digital at Marsh

WANNACRY

The NSA-Grade Stuxnet of Ransomware

$Billions

Ooops, your important files are encrypted.
NOTPETYA
If you already purchased your key, please enter it below.
Key:

Notpetya

Poisoned Source-code, NSA-Grade Worm meant to destroy

$1B for Maersk, Merck, FedEx

TAKING A STEP BACK

WE LIVE IN A WORLD OF EXTRAORDINARY CRIMES

WANNACRY

The NSA-Grade Stuxnet of Ransomware

$Billions

Ooops, your important files are encrypted.

If you already purchased your key, please enter it below.
Key:

NotPetya

Poisoned Source-code, NSA-Grade Worm meant to <u>destroy</u>

$1B for Maersk, Merck, FedEx

TAKING A STEP BACK

WE LIVE IN A WORLD OF EXTRAORDINARY CRIMES

Cyber crime damages will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015 – this represents the greatest transfer of economic wealth in history […] and is more profitable than the global trade of all major illegal drugs ($652B) and even all of counterfeiting ($1.13T) COMBINED

TAKING A STEP BACK

WE LIVE IN A WORLD OF EXTRAORDINARY CRIMES

“The aggregate cost of cyber is now estimated at over $1T a year of economic cost, verses roughly $300B experienced in 2017 lost to natural catastrophes"

- John Drzik, President of Global Risk and Digital at Marsh

FIVE FACTS FOR 2019 TO PUT THINGS IN PERSPECTIVE

1. Cyber Crime Costs – Will DOUBLE from $3T 2015 to $6T in 2021

2. Ransomware Costs – Up 15x since 2015, will be $11.5B by the end of the year, and increase 4x by 2020

3. Human Attack Surface – Will go from 3.8B people to 6B people by 2022

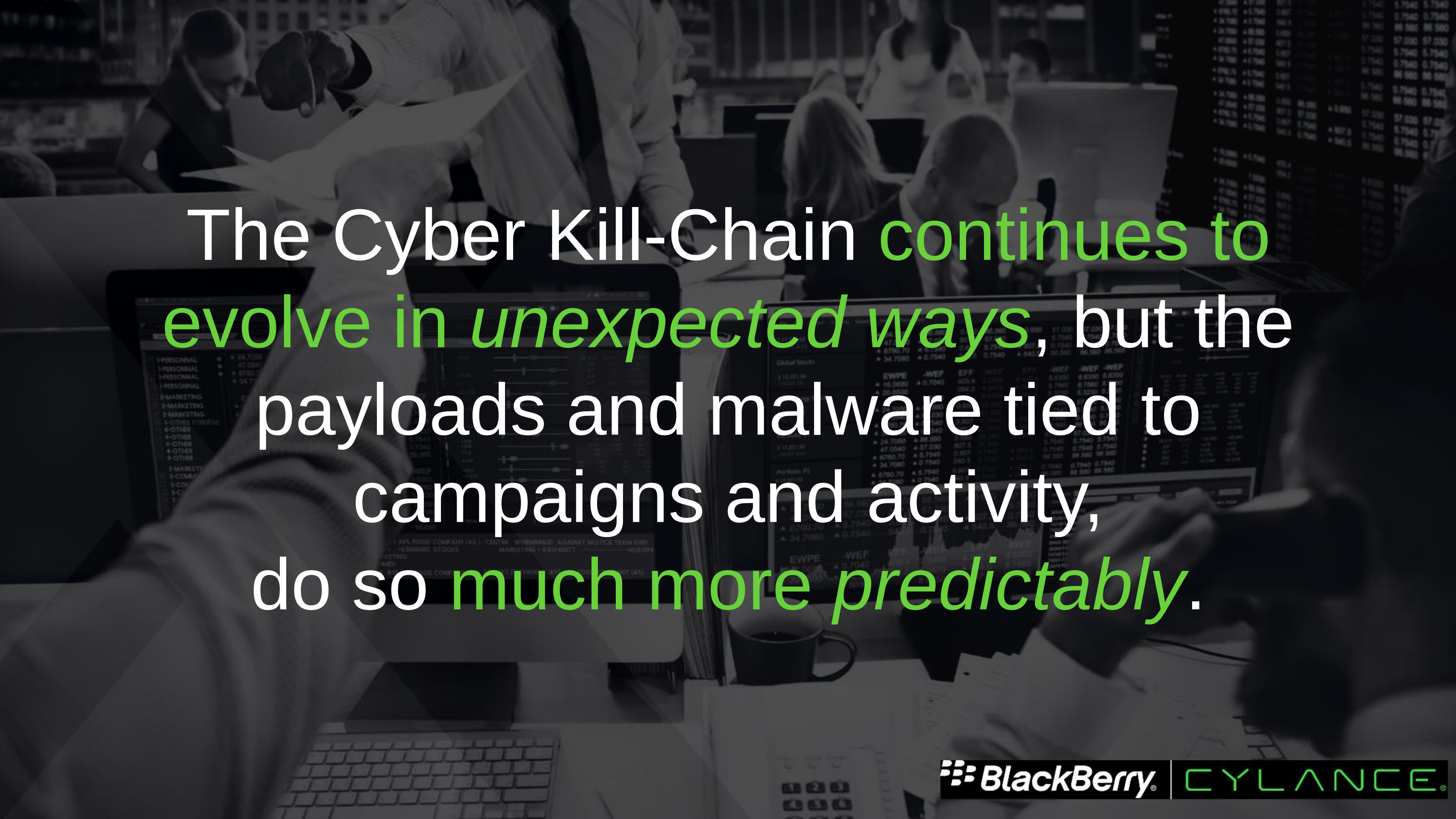
4. Unfilled Cyber Jobs – Will TRIPLE from 1.3m now (already zero U.R.) to 3.5m by 2021

5. Cyber Security Spending – Will go to $100B in 2017 to $1T by 2021

DEMO

EVOLVING TO PREVENTION

COME JOIN US –
WE HAVE A BETTER WAY



The Cyber Kill-Chain continues to evolve in *unexpected ways*, but the payloads and malware tied to campaigns and activity, do so much more *predictably*.

BlackBerry | CYLANCE

NETFLIX PREDICTIVE AI

IF TIME WAS A SPEAR…

KNOWN THREATS

UNKNOWN THREATS

AHEAD OF *ALL* THREATS

Legacy Antivirus

NG Firewalls / Air Gaps

Web Proxies

IDS/IPS

All Signature/Heuristic-Based Tech

Detonation Chambers,

Call-back Detection,

Anomalytics,

Cyber Threat Intelligence

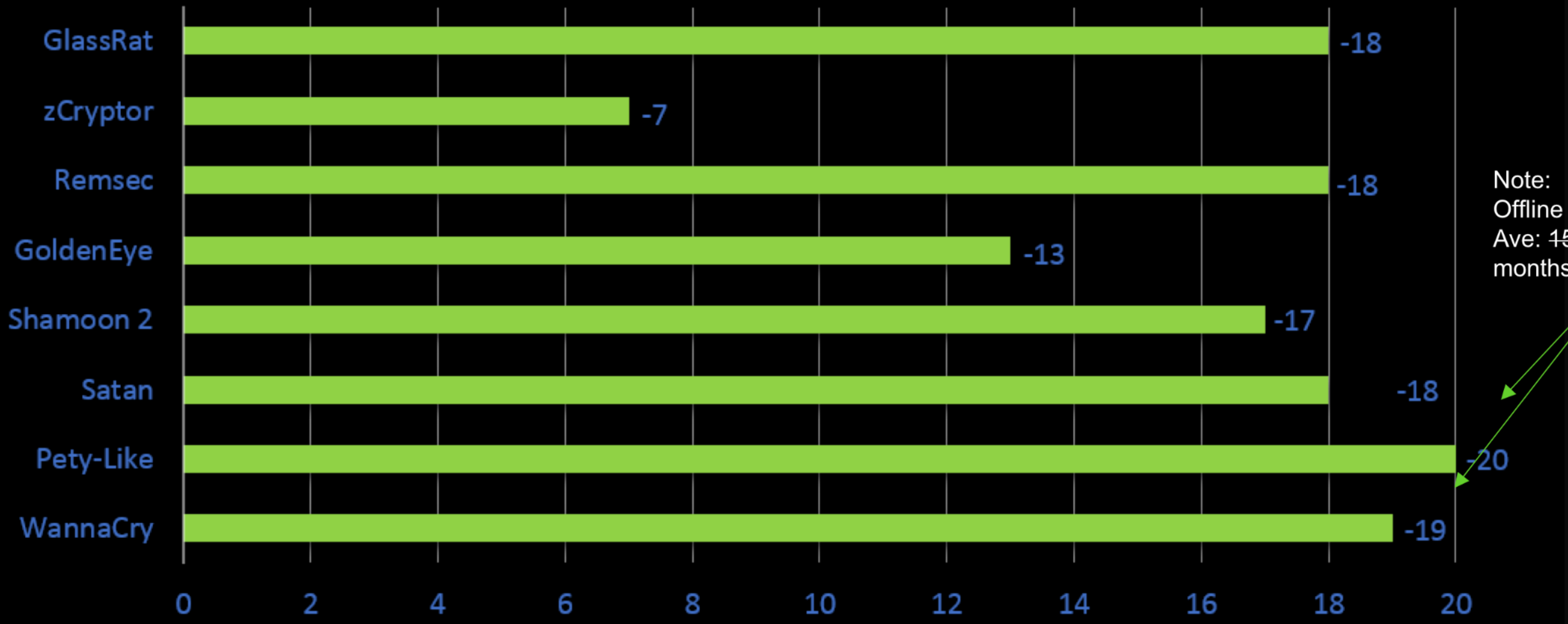
PREDICTIVE AI

TEMPORAL ADVANTAGE

To put it simply: threat actors have had a *time advantage* over us. We have been playing catch-up for decades.

PREDICTIVE AI'S TIME ADVANTAGE

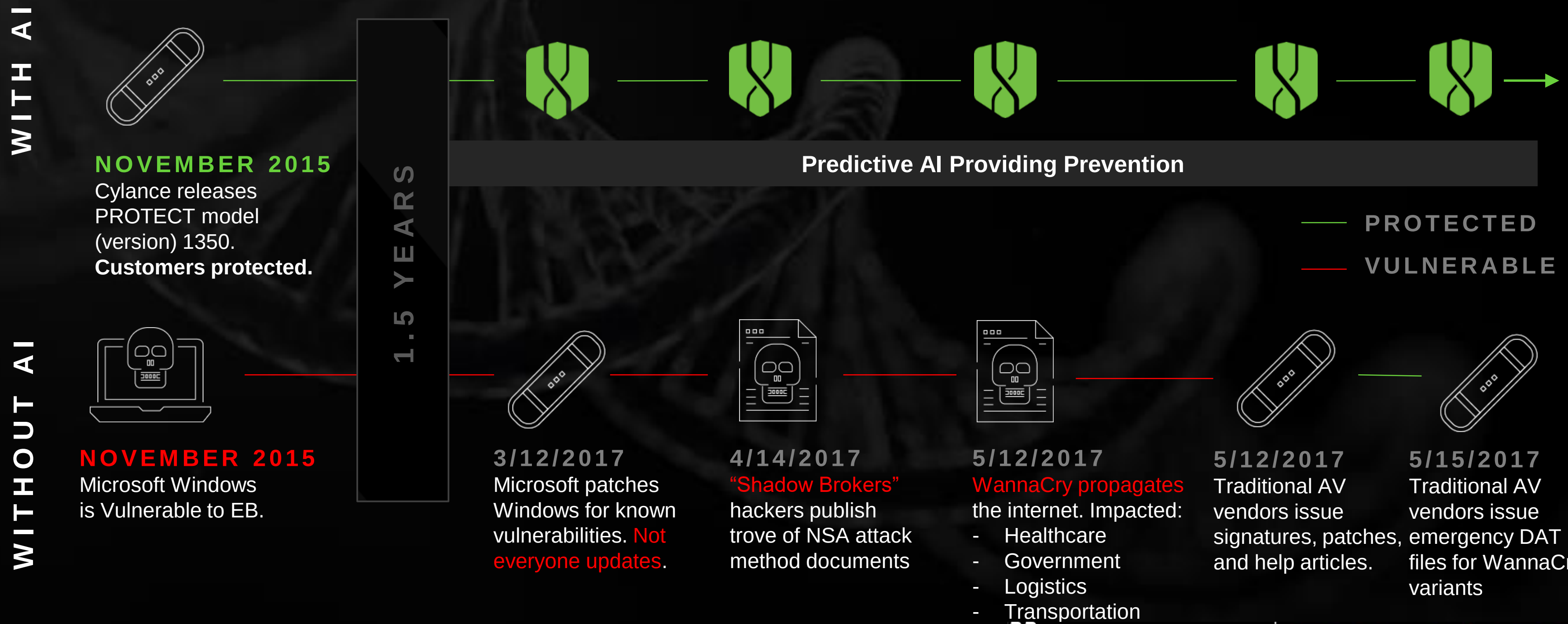
INITIAL RESEARCH



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

WHAT WE LEARNED FROM WANNACRY

CYLANCE PREDICTIVE ADVANTAGE



WITH AI

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

1.5 YEARS

Predictive AI Providing Prevention

PROTECTED

VULNERABLE

WITHOUT AI

NOVEMBER 2015
Microsoft Windows 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

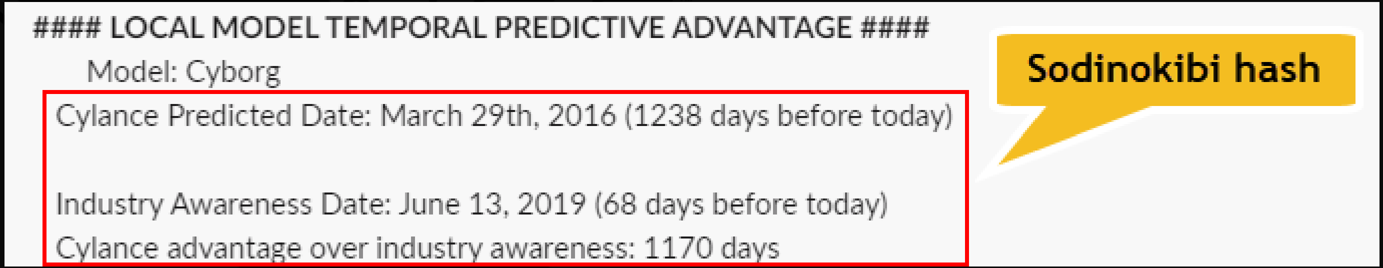
5/12/2017
WannaCry propagates the internet. Impacted:

- Healthcare
- Government
- Logistics
- Transportation

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

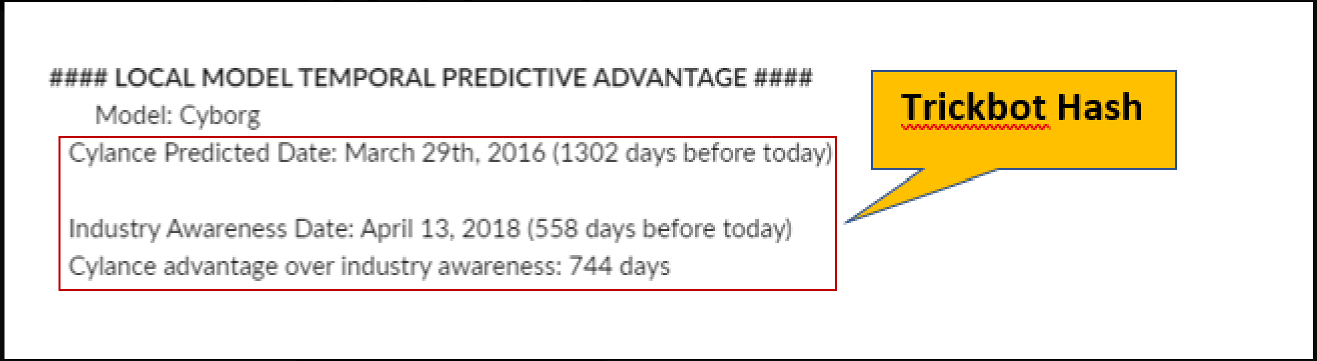
BlackBerry | CYLANCE



```
#### LOCAL MODEL TEMPORAL PREDICTIVE ADVANTAGE ####
    Model: Cyborg
  Cylance Predicted Date: March 29th, 2016 (1238 days before today)

  Industry Awareness Date: June 13, 2019 (68 days before today)
  Cylance advantage over industry awareness: 1170 days
```

Sodinokibi hash



LOCAL MODEL TEMPORAL PREDICTIVE ADVANTAGE

Model: Cyborg

Cylance Predicted Date: March 29th, 2016 (1302 days before today)

Industry Awareness Date: April 13, 2018 (558 days before today)

Cylance advantage over industry awareness: 744 days

BlackBerry® | CYLANCE®