Today

NUMBER OF SUCCESSFUL ATTACKS

COST OF LAUNCHING A SUCCESSFUL ATTACK
WE MUST CHANGE THE COST OF ATTACKS

NUMBER OF SUCCESSFUL ATTACKS

COST OF LAUNCHING A SUCCESSFUL ATTACK
THE ECONOMICS HAVE CHANGED

Available malware & exploits + Effective automated toolkits + Cheaper computing power = Successful data breaches

Adversary arithmetic
ATTACKERS ARE LAZY: TESLACRYPT

And mimics CryptoWall's dynamic library & function loading...

2013 - source code posted on Russian Forum And uses dynamic library & function loading...

Taken from Crypto locker And mimics CryptoWall Obfuscation from Carberp 2013

Imperative: leverage

ATTACKERS ARE LAZY:
IMPACT OF AUTOMATION

68 percent
Automated tools make it easier to execute attacks

64 percent
Tools are highly effective

63 percent
Increased usage of toolkits

$1,387
Spent on toolkits per attack
MASSIVE OVERLOAD

10,000+ events per month

64% duplicates

52% false positives

40% human inspection
Respondents believe that 39 percent of attacks can be prevented by shared intelligence.
AUTOMATED: YOUR VIEW
AUTOMATED: FOR ALL
IDENTIFYING 1 IN 7.4 BILLION

GLEN STEWART GODWIN

Unlawful Flight to Avoid Confinement - Murder, Escape

REWARD: The FBI is offering a reward of up to $100,000 for information leading directly to the arrest of Glen Stewart Godwin.

Hair: Black/Salt and Pepper
Eyes: Green
Complexion: Medium to Dark
Sex: Male
Race: White
Nationality: American

Glen Stewart Godwin is being sought for his 1987 escape from Folsom State Prison in California, where he was serving a lengthy sentence for murder. Later in 1987, Godwin was arrested for drug trafficking in Puerto Vallarta, Mexico. After being convicted, he was sent to a prison in Guadalajara. In April of 1991, Godwin allegedly murdered a fellow inmate and then escaped five months later.

Godwin is fluent in Spanish and may be traveling throughout Central and South America, and Mexico. He is thought to be involved in narcotics distribution.

https://www.fbi.gov/wanted/topten
THE “MAGIC”: CORRELATION

Exploit
Exploit_DNS_request
Exploit_Src_IP
Exploit_Protocol
Exploit_APP

Binary_Source
Binary_Protocol
Binary_MD5/SHA256
Bin_Digital_Sig
Binary_sys_changes

DNS_Req_Source
App_IP_request
App_Protocol
App_Protocol_CMD
App_Protocol_Encryption

Gather Intelligence
Leverage Exploit
Execute Malware
Control Channel
Steal Data
THREAT SHARING: INDUSTRY COOPERATES

CYBER THREAT ALLIANCE

FOUNDING MEMBERS

- Palo Alto Networks
- Symantec
- Fortinet
- McAfee
- TAXII
- STIX
- CybOX

...
Increasing the time to breach an organization by less than 2 days deters 60% of attacks.
1. **Share** intelligence with your security partners

2. **Collaborate** in industry communities
   - Industry – FS-ISAC
   - National – CISP
   - Vendor – Cyber Threat Alliance

3. We have the **CPU** power to turn the scales: the **cloud**

4. Kill the whole **attack lifecycle**, not just the attack binary

5. Integrated & automated security **platforms** are the enemy of the attacker
Palo Alto Networks Academy Overview

- **Purpose**
  - The Palo Alto Networks Academy is designed to equip students with the next-generation cybersecurity knowledge they’ll need to succeed in today’s rapidly changing cyber-threat landscape.

- **Who & Where?**
  - 160+ Authorized Academy Centers (AACs) in 20 countries (as of January 2017)
  - Any degree-granting, nationally accredited university or college

- **Academy Benefits**
  - Faculty training (TTT) at no cost
  - Training lab support at no cost
  - Courseware at no cost
  - PCNSE certification vouchers at 50% discount

- **How?**
  
  www.paloaltonetworks.com/academy