Cyber Threat Landscape

Robinson J, Agilan N Herald

***Abstract*:- The Security Threat Landscape Has Been Exciting And Surprising. We Will Presents The Best Predictions On How The Threat Will Change In Attacking Your Enterprise. It Provides An Overview Of Threats, Together With Current And Emerging Trends. It Is Based On Publicly Available Data And Provides An Independent View On Observed Threats, Threat Agents And Threat Trends. Understanding The Forces That Shape The Threat Landscape Is Essential For Financial Institutions To Get Ahead And Stay Ahead Of Their Adversaries In Cyberspace.**

Key Words:* *Cyber security, Threat landscape, Risk, Cyber defenses, Cyber attack

I. INTRODUCTION

This paper will descent into the latest tools, techniques and threats developed and utilized by cybercriminals. The paper will include a market overview of the latest offerings from the criminal underground, with a deep descent into some of the techniques discussed by cybercriminals and a review of how they manifest as attacks with real world examples and case studies. A share of the presentation will also be dedicated to possible mitigation strategies and techniques.

II. STRATEGIC PLANNING ASSUMPTION (SPA)

By 2020, a third of successful attacks experienced by enterprises will be on their shadow IT resources

Through 2020, 99% of vulnerabilities exploited will continue to be the ones known by security and IT professionals for at least one year.

Strategic Technology Trends:

Intelligent: Artificial Intelligence and Advanced Machine Learning**,** Intelligent Apps, Intelligent Things

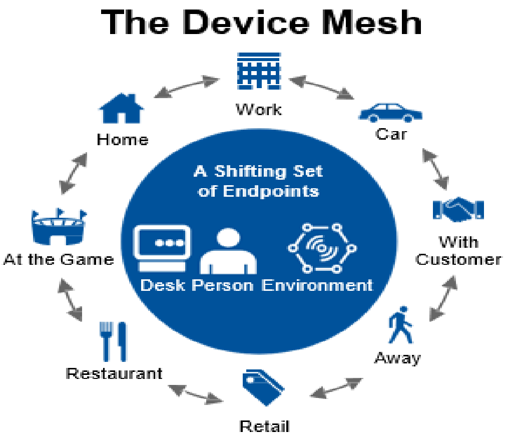
Digital: Virtual Reality and Augmented Reality, Digital TwinsBlockchains and Distributed Ledgers

Mesh: Conversational Systems, Digital Technology Platforms, Mesh App and Service Architecture, Adaptive Security Architecture

Strategic Planning Assumption

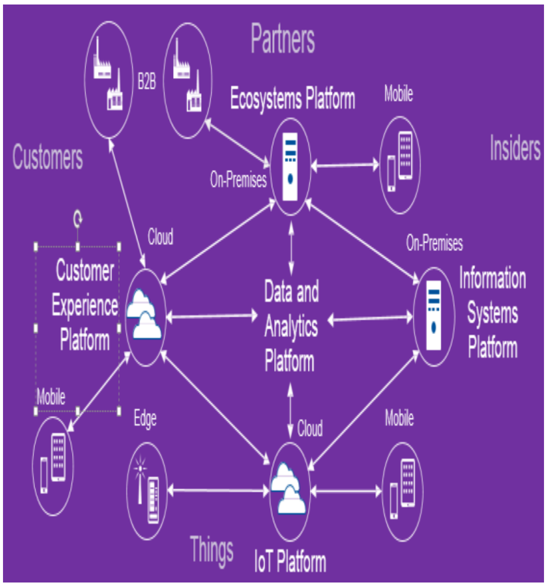
"The Death of Least Privilege"

Your IT Is More Complex, but More Connected



Complexity and Heterogeneity Are the Enemies of Security

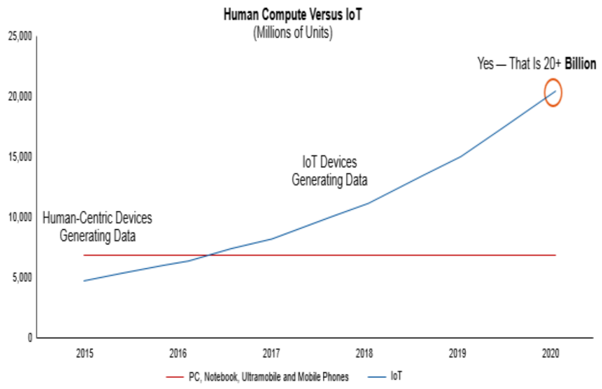
All Your Stuff Is Not Under One Roof



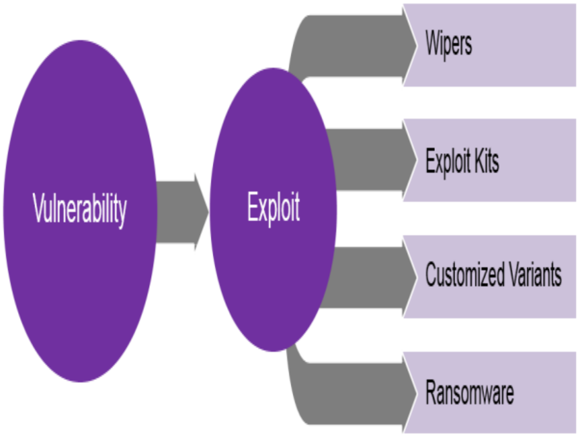
IoT Are Sprinklers

Endpoints of the Internet of Things will grow at a 32.9% CAGR from 2015 through 2020, reaching an installed base of 20.4 billion units.

In 2020, 6.5 billion "things" will ship, with 64% of them being consumer applications.Total spending on endpoints and services will reach $3.4 trillion in 2020.



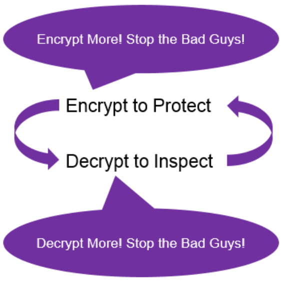
The Force Multiplier of New Exploit Families



Encryption Remains Under Pressure

MD5 Encryption will always be mentioned when going over the topic of cryptography. Message-Digest algorithm 5, more commonly known as MD5, is a type of cryptographic hash function that is generally used together with a 128-bit hash value.

SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest - typically rendered as a hexadecimal number, 40 digits long.


Encrypt More! Stop the Bad Guys!
Encrypt to Protect
Decrypt to Inspect
Decrypt More! Stop the Bad Guys!

MD5 Proven Theoretically Pre-Stuxnet Flame Used MD5 Collide

SHA-1 Collision Attack Proved Clock Is Ticking

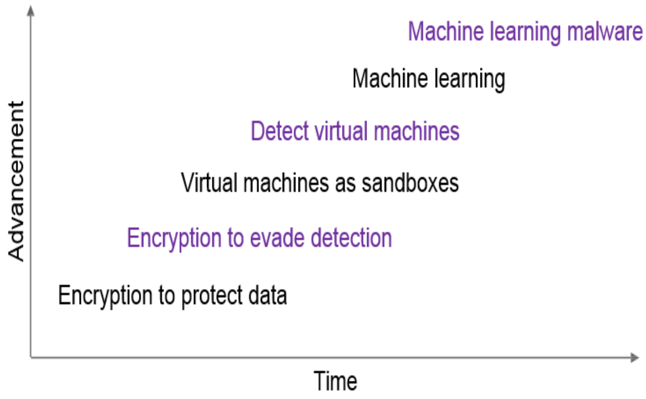
Machine Learning

The iterative aspect of machine learning is important because as models are exposed to new data, they are able to independently adapt. They learn from previous computations to produce reliable, repeatable decisions and results. It's a science that's not new – but one that has gained fresh momentum

Machine Learning Is a Technique, Not the Objective

- ✓ A lot of hype.
- ✓ Use quality metrics to evaluate the outcome, not the technique:
  - – Anomaly detection: detection and false positive rate
  - – Security analytics: use SOC analyst productivity metrics
- ✓ Using new techniques does not necessarily equal better detection:
  - – Anomaly detection can be achieved with allegedly more basic techniques:
    - ▪ Reputation and fingerprinting: if the attacker is known
    - ▪ Pattern matching and heuristics: if the attack technique is known
    - ▪ Whitelisting: if the expected behavior is known (and consistent)

Machine Learning Won't Be the Answer


Machine learning malware
Machine learning
Detect virtual machines
Virtual machines as sandboxes
Encryption to evade detection
Encryption to protect data
Advancement
Time

III. EXPLOIT KITS

Top toolkits used to exploit system vulnerabilities

SofosFO/Stamp Exploit Kit : The exploit kit, also known as GrandSoft, uses compromised websites to infect users with browser vulnerabilities containing Flash or Java components. The exploit kit is used to infect victims with ransomware, miners, and various Trojans.

Neutrino Exploit Kit : Neutrino and its predecessor Neutrino-v are popular exploit kits that surged in mid-2016. They are known for using compromised sites and malvertising to infect users with various malware.

Empire Pack Exploit Kit : The exploit kit, also referred to RIG-E, surfaced in September 2016 and takes advantage of flaws in Microsoft and Adobe software.

Magnitude Exploit Kit : Also known as Popads, Magnitude is used in malvertising attacks to infect victims who visit compromised websites.

CAMPAIGNS

Top targeted attacks

Operation ZooPark : The campaign focuses on users in the Middle East in an attempt to infect Android devices with malware. The threat actors behind the operation mainly use waterhole attacks to infect victims to steal sensitive information. The attacks date back to at least 2015 and have been known to also use Telegram channels to infect users.

Operation VPNFilter : The attack focuses on networking equipment from various vendors as well as network-attached storage (NAS) devices. The malware used in the campaign has the ability to steal sensitive information and make infected devices unusable. Equipment affected includes those from Linksys, MikroTik, NETGEAR, TP-Link, and QNAP.

Operation Prowli : The campaign targets a range of platforms in an attempt to carry out traffic-hijacking and cryptomining. The operation has affected thousands of devices including IoT, modems, and web servers for financial gain.

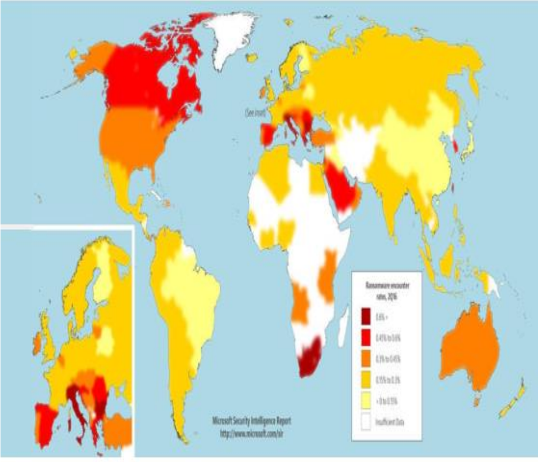
Operation InvisiMole : The campaign consist on two main backdoor components used to spy on its victims in an attempt to steal sensitive information. The malware used in the operation has the ability to record audio using the computer's microphone as well as take screenshots using the system's camera.

Operation HyperBro : The threat actors behind the campaign used the HyperBro RAT in the last stage of the attacks to gain access to the infected systems. The operation targeted organizations associated with the government in an attempt to steal sensitive information.

Operation MirageFox : The campaign used an updated version of a RAT known as Mirage that dates back to at least 2012. The operation focuses on exfiltrating data from the victim including computer name, cpu information, and username and sends the data back to C2 servers under the attackers control.

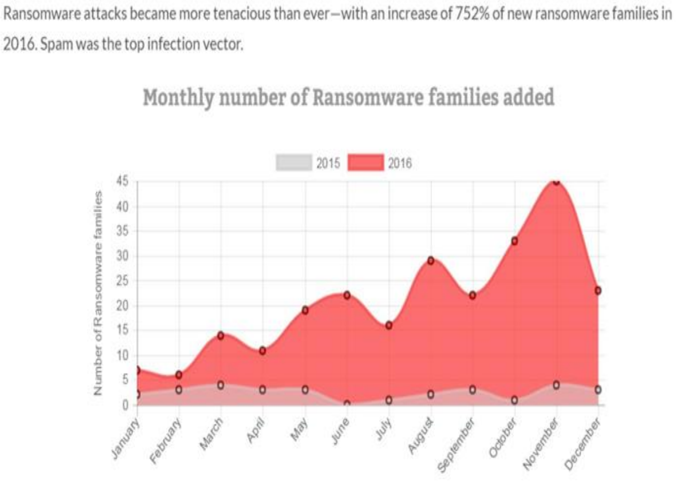
RANSOMWARE

A type of malicious software designed to block access to a computer system until a sum of money is paid.

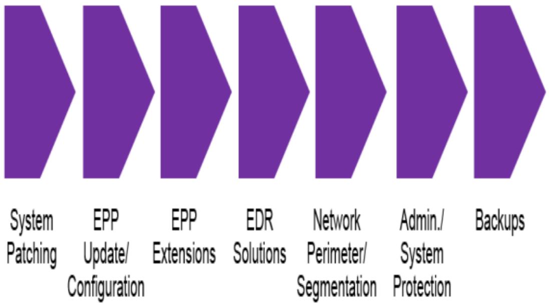

Ransomware encounter rates, 2016
0.6% +
0.45% to 0.6%
0.3% to 0.45%
0.15% to 0.3%
> 0 to 0.15%
Insufficient Data
Microsoft Security Intelligence Report
http://www.microsoft.com/sir

Ransom ware Weather Mapping

Ransomeware Growth is Not Hype

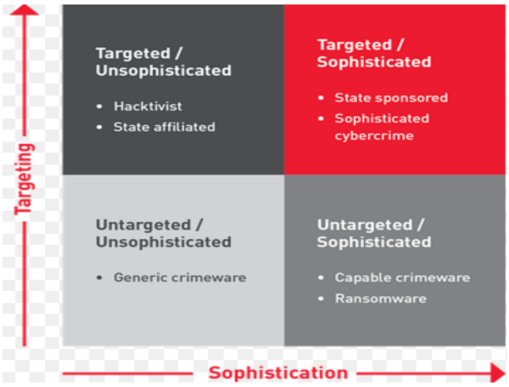

Ransomware attacks became more tenacious than ever—with an increase of 752% of new ransomware families in 2016. Spam was the top infection vector.

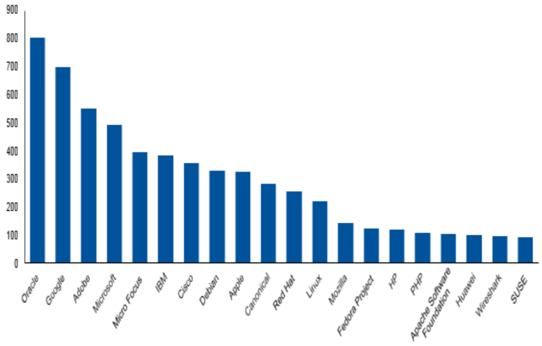
Prevent Ransomware


System Patching
EPP Update/ Configuration
EPP Extensions
EDR Solutions
Network Perimeter/ Segmentation
Admin./ System Protection
Backups

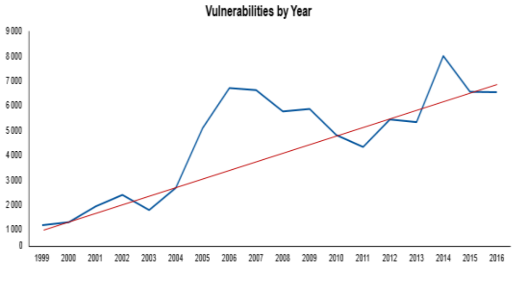
STATE SPONSORED THREAT & VULNERABILITIES

- Almost all enterprises should treat state threats as part of usual advanced threats.
- Certain verticals and industries do need to take more focused actions.
- State-sponsored attack teams in many countries "free-lance" after hours. Techniques will be the same, but the targeting and level of stealthiness will differ.
- Don't hack back. Unless you are the state. And maybe not even then.
- Don't neglect best-practice level safeguards to focus on more advanced attacks.



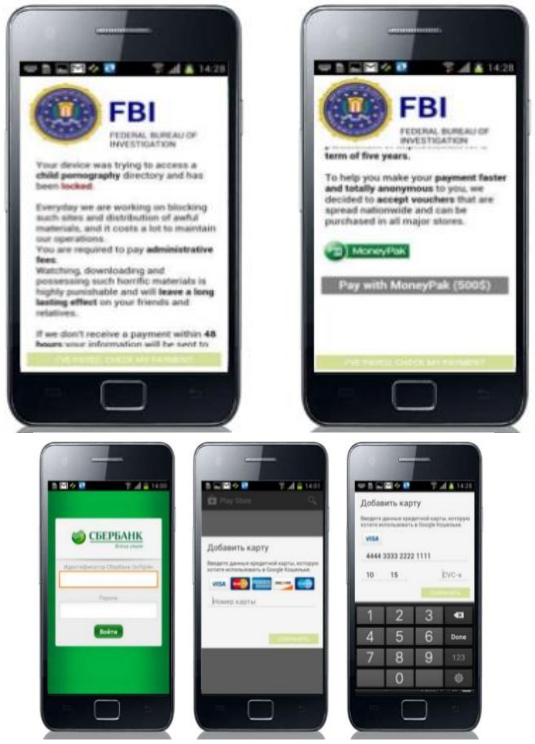


Top 20 Distinct Vulnerabilities by Vendor



We're Not Even Looking at All the Roofs

Your Roofs Are Leaky, and Getting Leakier
NEW MOBILE THREATS


FBI
FEDERAL BUREAU OF INVESTIGATION

Your device was trying to access a **child pornography** directory and has been **locked**.

Everyday we are working on blocking such sites and distribution of awful materials, and it costs a lot to maintain our operations.
You are required to pay **administrative fees**.
Watching, downloading and possessing such horrific materials is highly punishable and will **leave a long lasting effect** on your friends and relatives.

If we don't receive a payment within **48 hours** your information will be sent to

I'VE PAYED, CHECK MY PAYMENT

FBI
FEDERAL BUREAU OF INVESTIGATION

term of five years.

To help you make your **payment faster and totally anonymous** to you, we decided to **accept vouchers** that are spread nationwide and can be purchased in all major stores.

MoneyPak

Pay with MoneyPak (500$)

I'VE PAYED, CHECK MY PAYMENT

Mobile Ransomware Overlay Mobile Attack

IV. CONCLUSION

- Stop Counting Threats
- Stop Scaring Scared People Use Your Humans Wisely
- Patch Your Things, Do Your Best
- Watch the Weather: Keep Detecting
- Plan for Future Trends Now
- Fix That Leaky Roof

REFERENCES

For more information please visit:
[1].https://www.gartner.com/en,
[2].http://www.mcafee.com,
[3.]http://www.trendmicro.com
[4].etl.enisa.europa.eu