Advanced Endpoint Protection

Scottie Wang 王信強

Technical Consultant

paloalto NETWORKS®

v1.0 – May

Old School.....

Old School.....

Old School.....

Attackers....

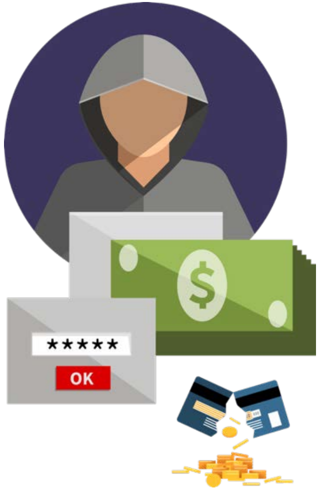
Attackers....

Approach...

Demo

Attackers need to control the endpoint

Attackers objectives require leveraging the endpoint



RAPIDLY CHANGE & MORPH MALWARE

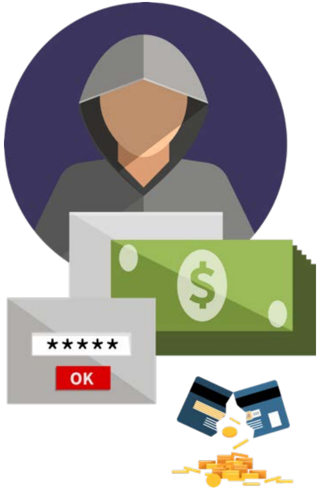
EXECUTE MALWARE

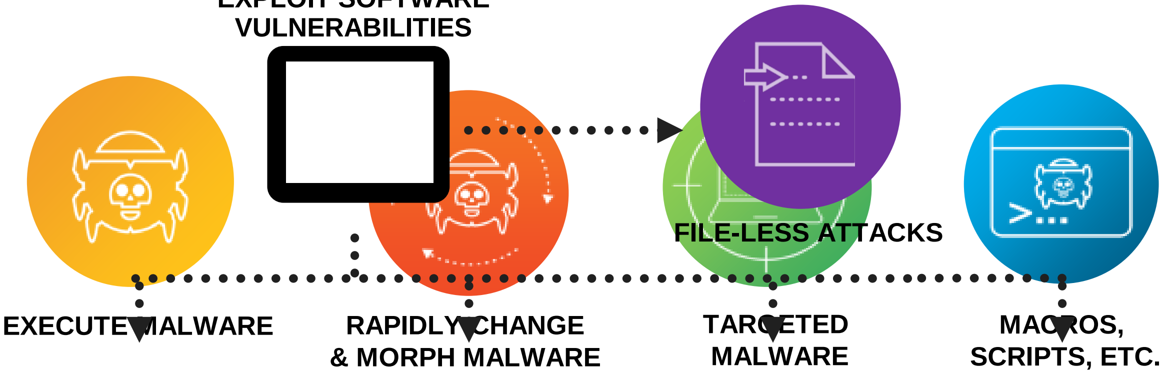
TAILORED MALWARE

SCRIPTS, ETC.

Attackers need to control the endpoint

Attackers objectives require leveraging the endpoint





Other solutions optimize for only one aspect…

Signature-based solutions **can’t prevent unseen malware**

Machine learning solutions **cannot detect targeted malware**

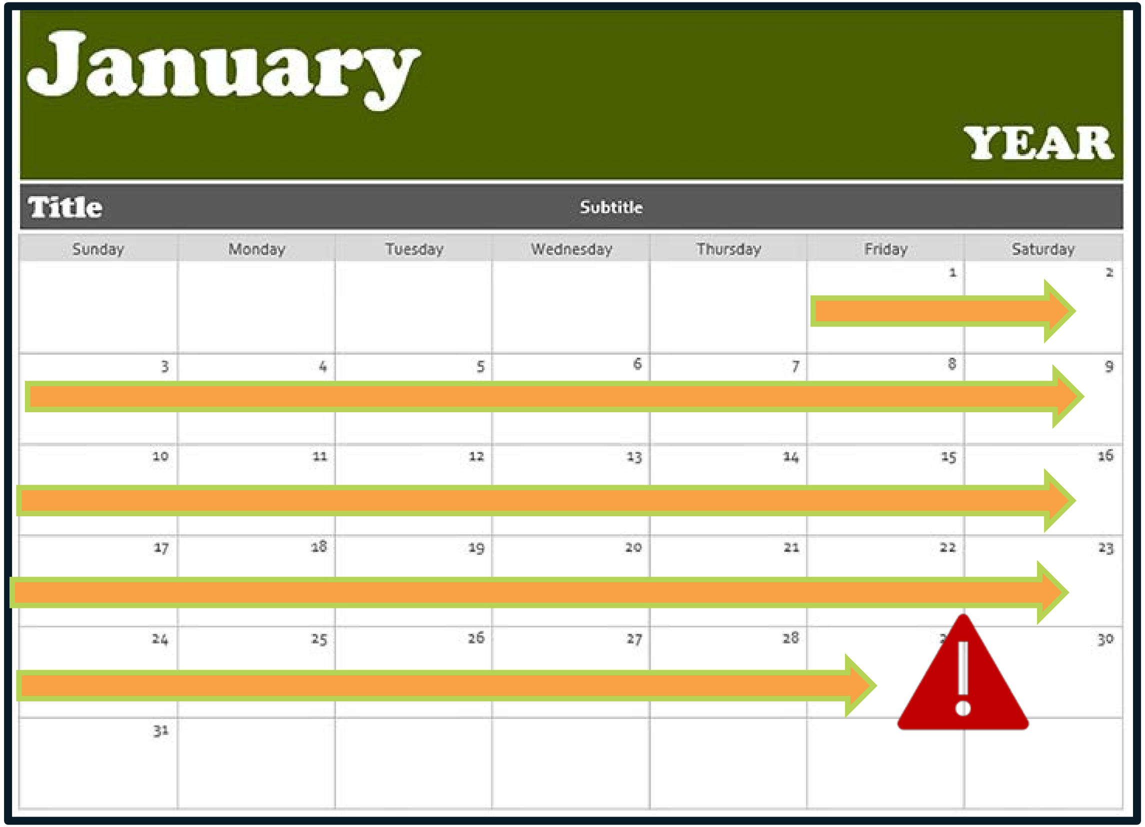
Most solutions have **minimal, if any, exploit prevention** capabilities

Detection **causes event and IR overload**

Time to Business Impact of Modern Attacks

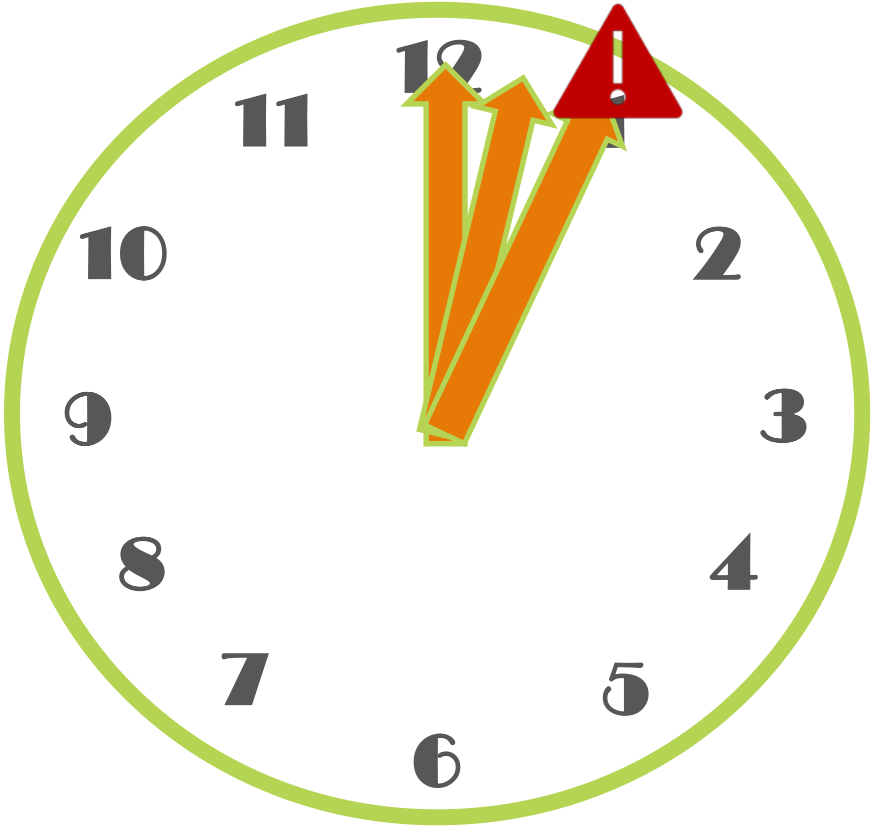
There used to be time to:

- Scan
- Get Signature Updates
- Invoke EDR and assign a couple employees to fix the few issues…

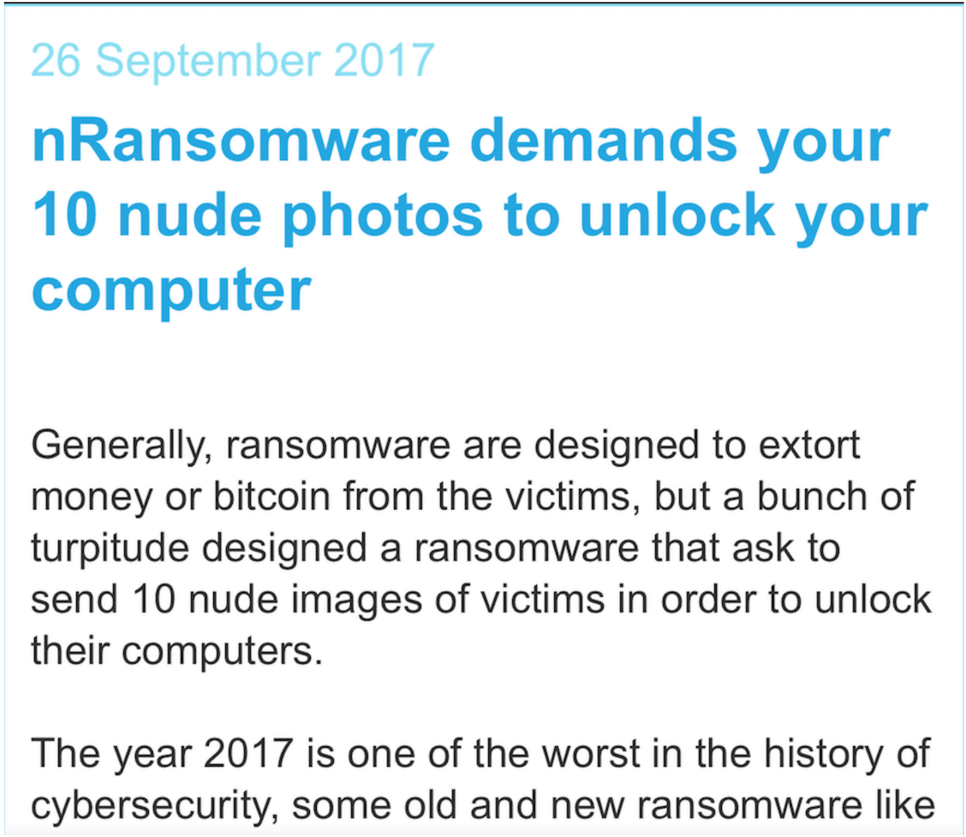


Time to Business Impact of Modern Attacks

- **Ransomware does not take days…**
- **Far too fast for manual response or human interference**
- **Your machines still got locked**
- **Morphing makes every situation potentially patient-zero**
- **Signature updates leave large windows of vulnerability**



Recent Trend of Ransomware

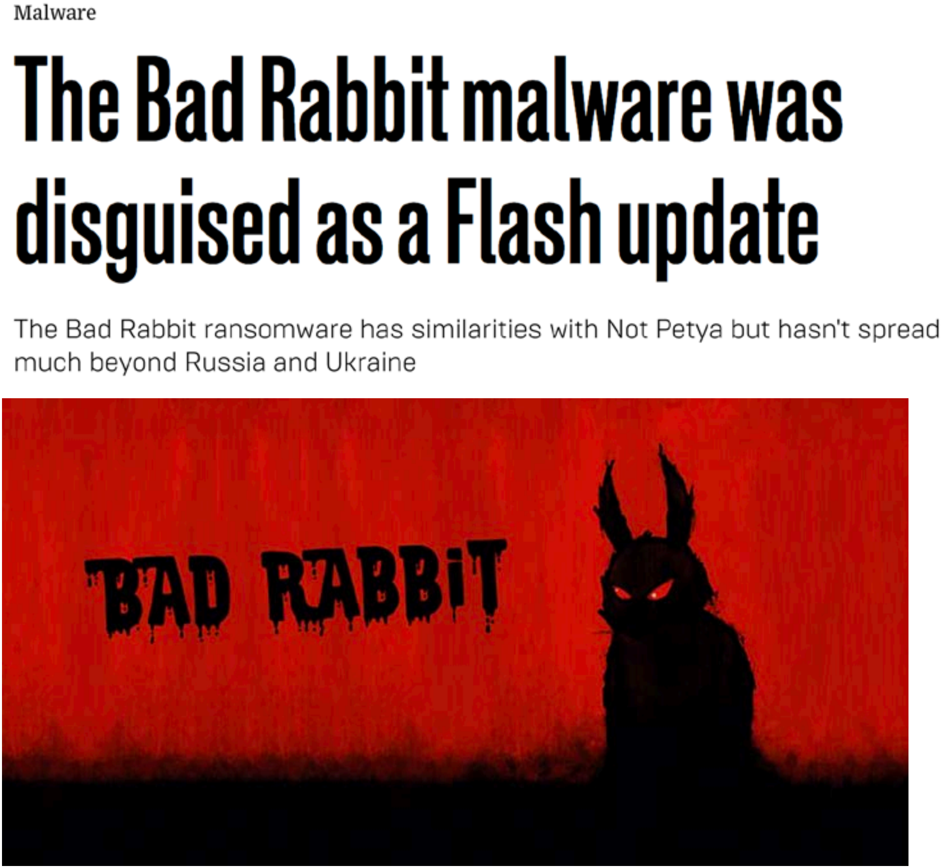


26 September 2017

nRansomware demands your 10 nude photos to unlock your computer

Generally, ransomware are designed to extort money or bitcoin from the victims, but a bunch of turpitude designed a ransomware that ask to send 10 nude images of victims in order to unlock their computers.

The year 2017 is one of the worst in the history of cybersecurity, some old and new ransomware like

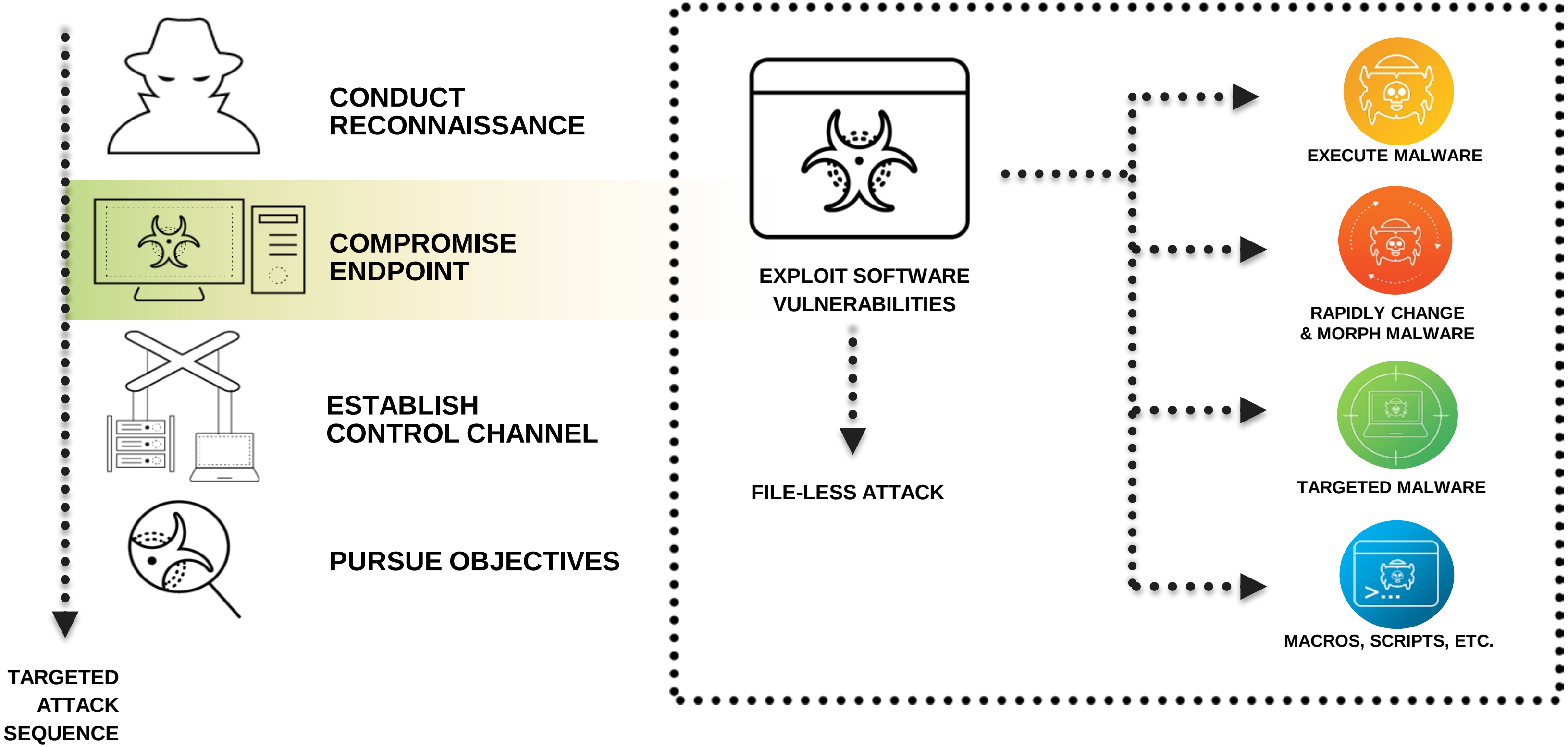


Malware

The Bad Rabbit malware was disguised as a Flash update

The Bad Rabbit ransomware has similarities with Not Petya but hasn't spread much beyond Russia and Ukraine

The Need For A Multi-Method Prevention Approach



Block the Core Techniques, Not the Individual Attacks

Number of New Variants

Individual Attacks

Thousands

Software Vulnerability Exploits

Thousands of new vulnerabilities and exploits per year

Core Techniques

0 – 1

Exploit Techniques

Zero to one new exploit techniques per year

Millions

Malware

Millions of new malware variations per year

Few

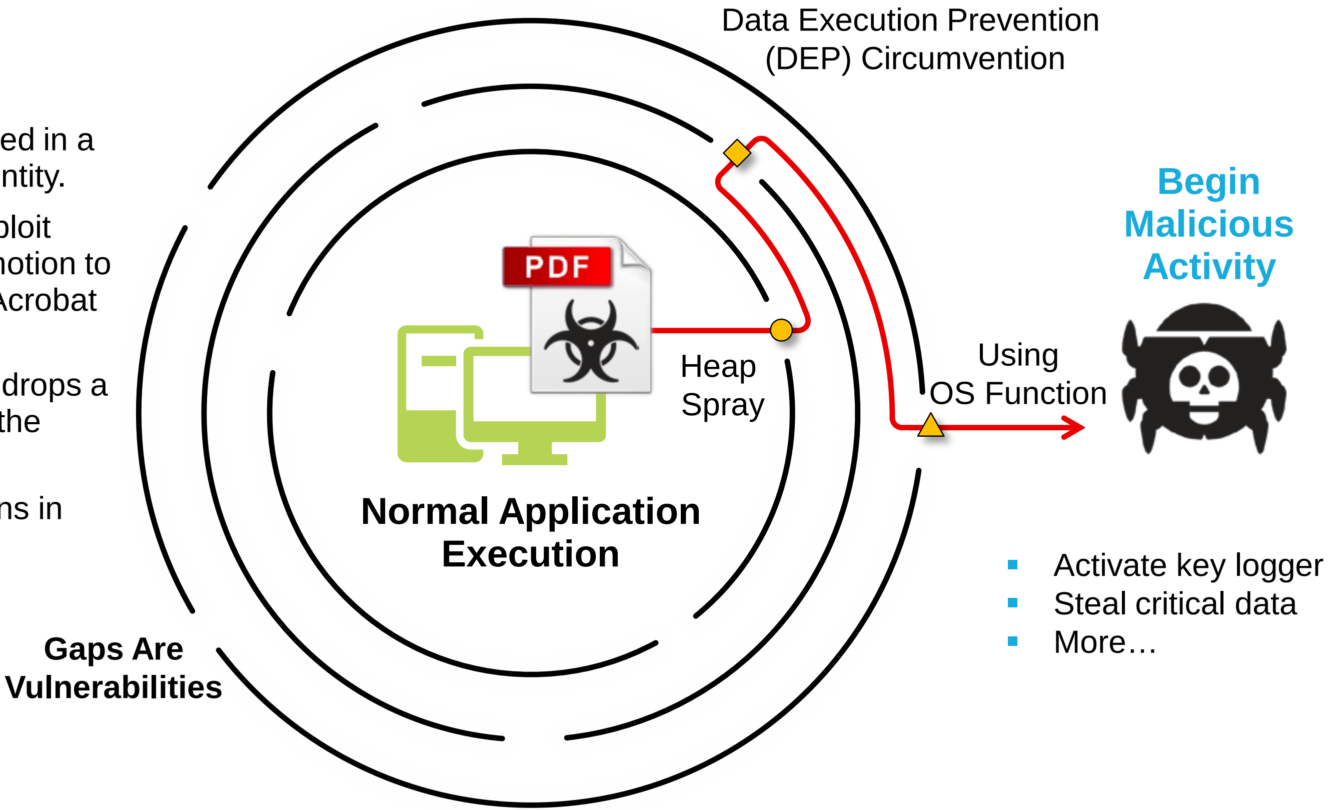
Malware Techniques

A handful of malware approaches per year

Application Exploit Techniques

Exploit Attack

1. Exploit attempt contained in a PDF sent by “known” entity.
2. PDF is opened and exploit techniques are set in motion to exploit vulnerability in Acrobat Reader.
3. Exploit evades AV and drops a malware payload onto the target.
4. Malware evades AV, runs in memory.

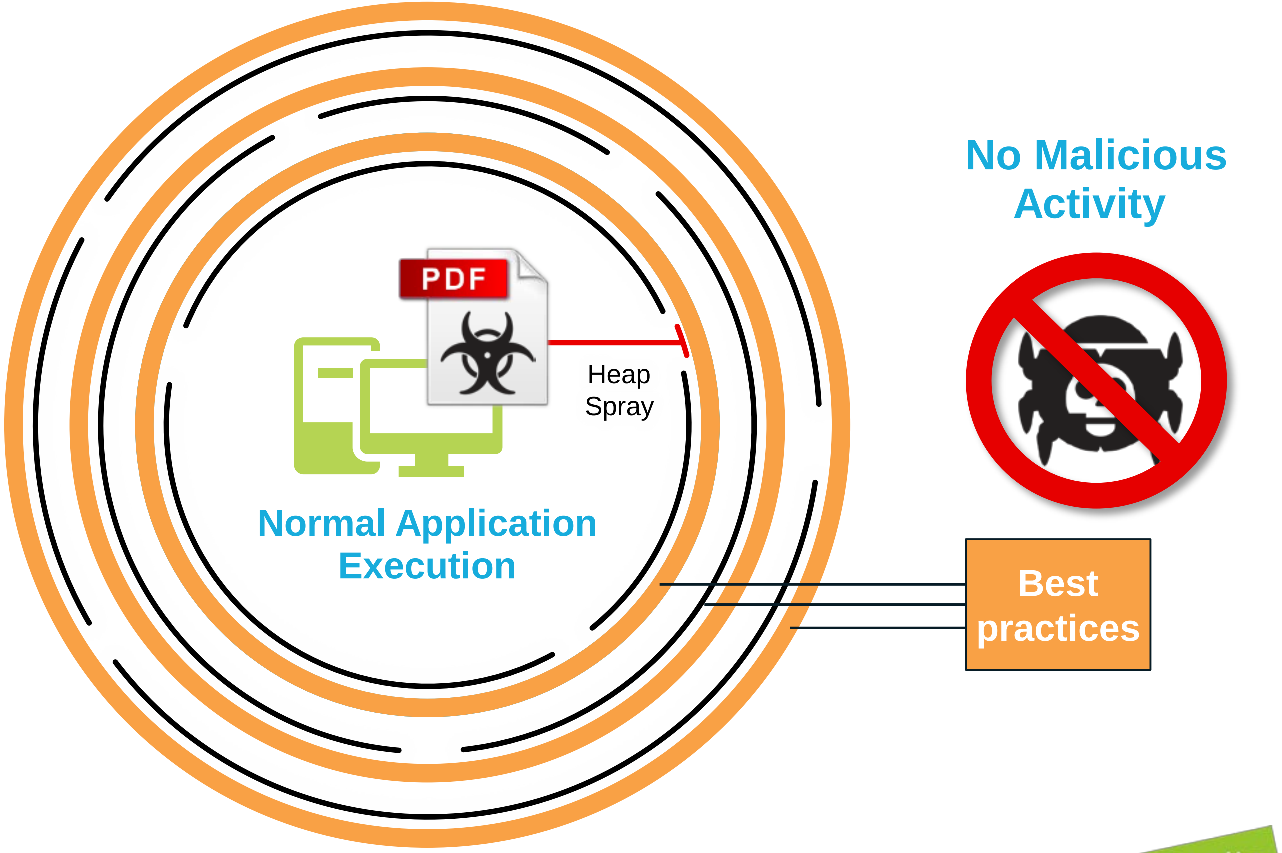


- Activate key logger
- Steal critical data
- More…

Application Exploit Techniques (Cont.)

Exploit Attack

1. Exploit attempt contained in a PDF sent by “known” entity.
2. PDF is opened and exploit techniques are blocked by Traps.



Heap Spray

Normal Application Execution

No Malicious Activity

Best practices

Shutdown Attackers with Integrated Remediation

Magna Enables You to Block or Quarantine Users or Devices

Terminate
Malicious Files (MFT)

Block Malicious
Domains with NGFW

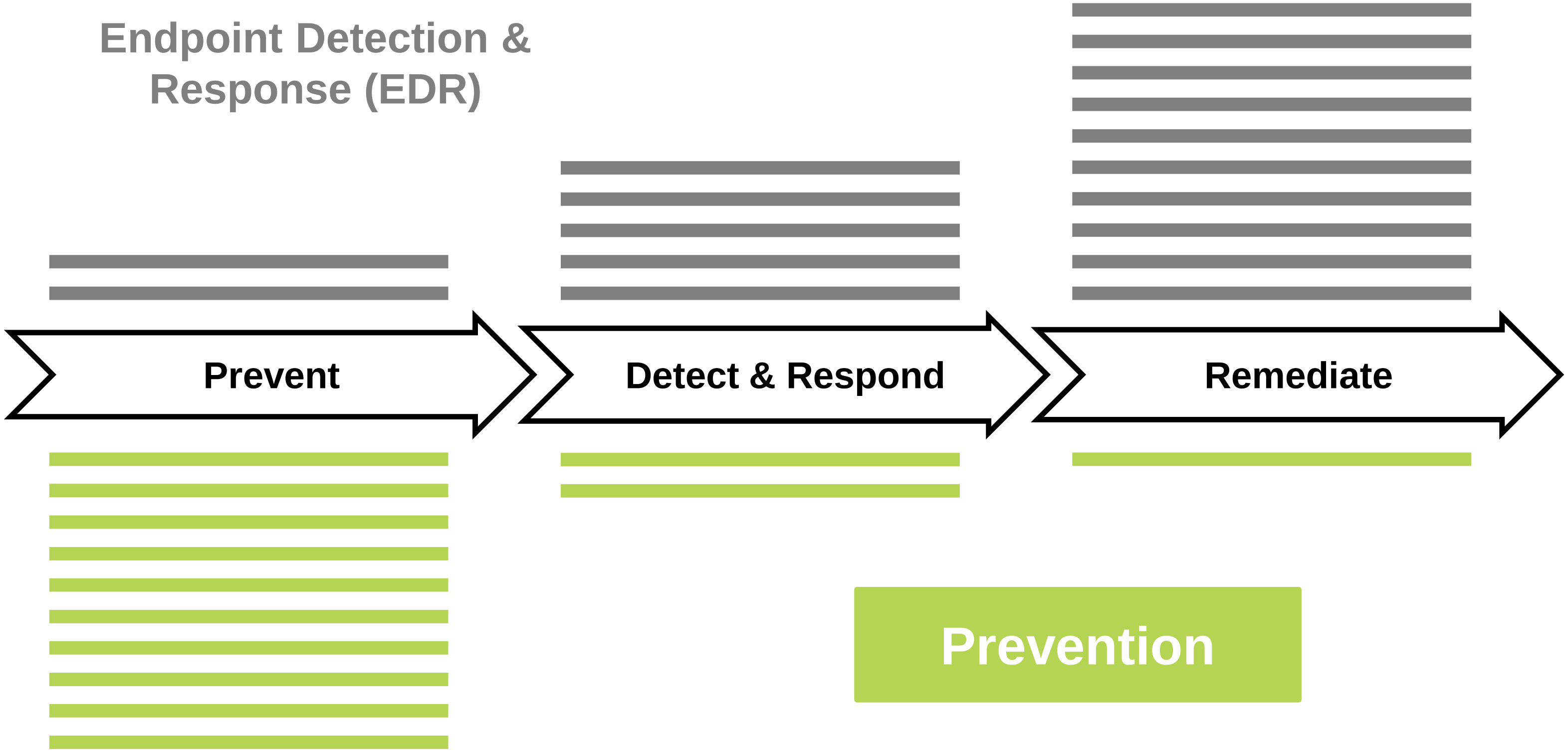
Isolate Infected
Machines With NGFW

Isolate Infected
Machines with NAC

Lock Accounts
in Active Directory

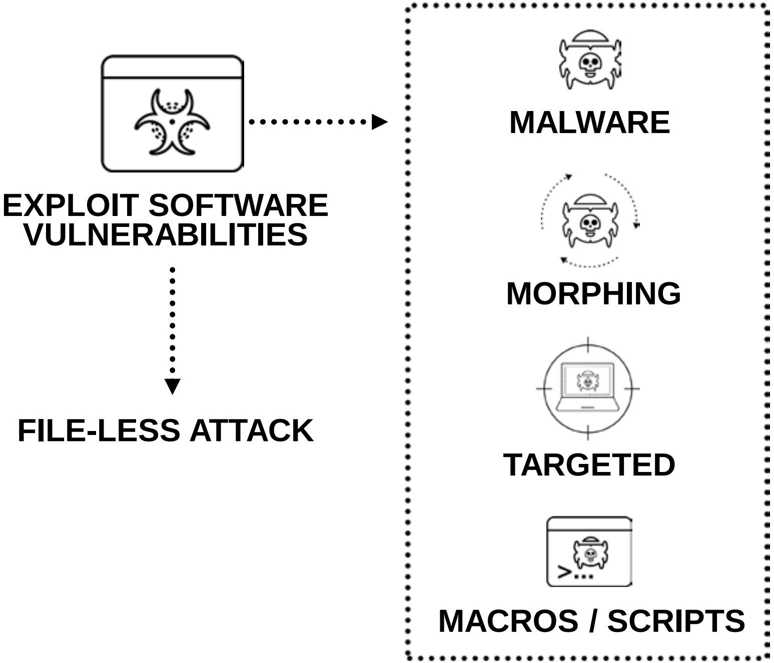
Reset Compromised
AD Passwords

You should be focusing on Prevention



Prevention

Multi-Method Malware Prevention



EXPLOIT SOFTWARE VULNERABILITIES

FILE-LESS ATTACK

MALWARE

MORPHING

TARGETED

MACROS / SCRIPTS

REDUCE THE ATTACK SURFACE
Policy Controls, Child Processes, Execution Restrictions

PREVENT KNOWN MALWARE
WildFire Threat Intelligence

PREVENT UNKNOWN MALWARE
Local Analysis via Machine Learning

DETECT ADVANCED THREATS
WildFire Inspection & Analysis

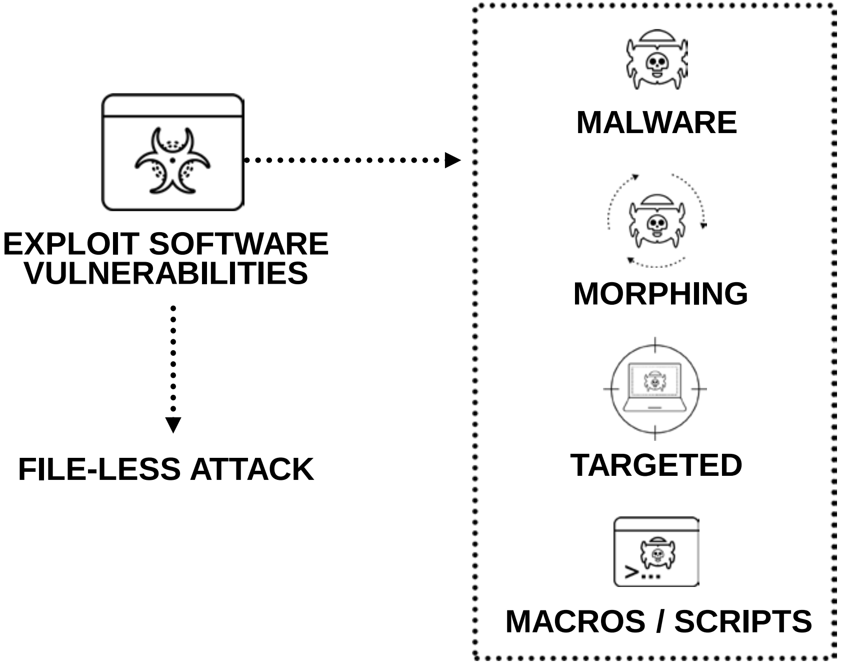
Multi-Method Exploit Prevention

RECONNAISSANCE PREVENTION

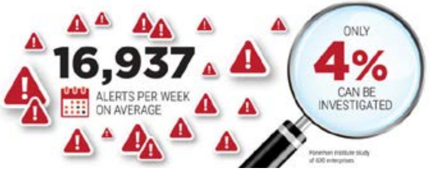
MEMORY CORRUPTION PREVENTION

CODE EXECUTION PREVENTION

KERNEL PROTECTION



Lower Operating Costs with Accurate, Efficient Alerts



Most IT security teams can't keep up with the deluge of security alerts

LIGHTCYBER ACCURACY

61%

ACROSS
ALL ALERTS

99%

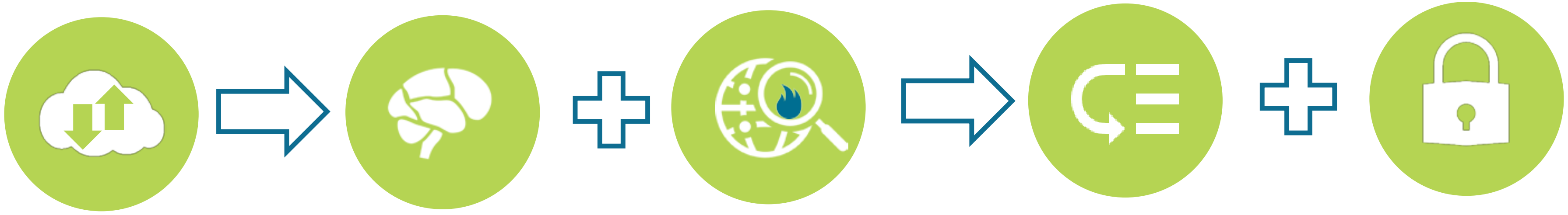
ACROSS MAGNA'S
AUTOMATED "CONFIRMED
ATTACK" CATEGORY

EFFICIENCY

0.9 alerts / 1K endpoints / day

Source: Ponemon survey of 700 enterprises with average 14,000 endpoints and 16,937 alerts per week

Multi-Method Malware Prevention



Threat Intelligence

Prevents Known Threats

Local Analysis

Prevents Unknown Threats

Dynamic Analysis

Detects Advanced Unknown Threats

Malicious Process Prevention

Prevents Script-Based & File-Less Threats

Ransomware Protection

Additional Ransomware Protection

Multi-Method Exploit Prevention

Reconnaissance Protection

Automatic Prevention of Vulnerability Profiling Used by Exploit Kits

+

Technique-Based Exploit Prevention

Blocking of Exploit Techniques Used to Manipulate Good Applications

+

Kernel Protection

Protection Against Exploits Targeting or Originating from the Kernel

Data Center

Data Center

The Cloud

Hybrid..

Thank You