Advanced Endpoint Protection

Scottie Wang 王信強

Technical Consultant

Old School.....

Old School.....

Old School.

Old School.....

Attackers....

Attackers….

Attackers....

Attackers….

Attackers….

Approach...

Demo

Attackers need to control the endpoint

Attackers objectives require leveraging the endpoint

RAPIDLY CHANGE & MORPH MALWARE

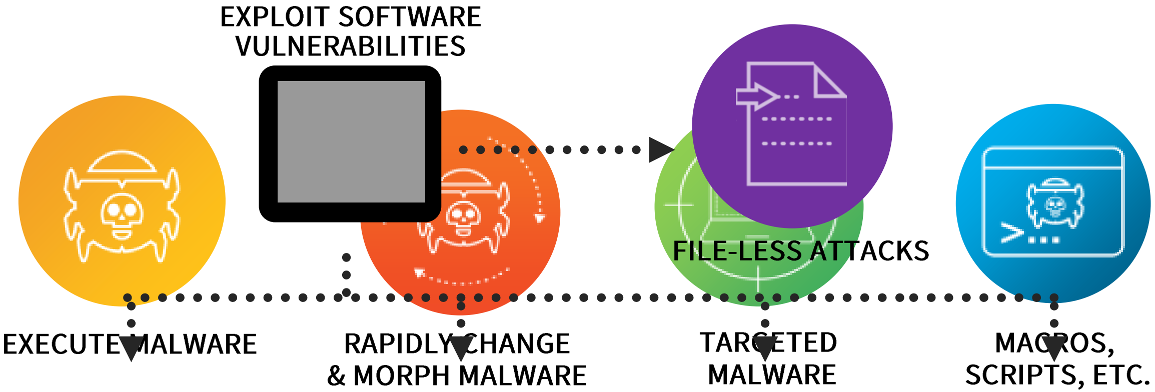
EXECUTE MALWARE

MACROS, SCRIPTS, ETC.

MALWARE

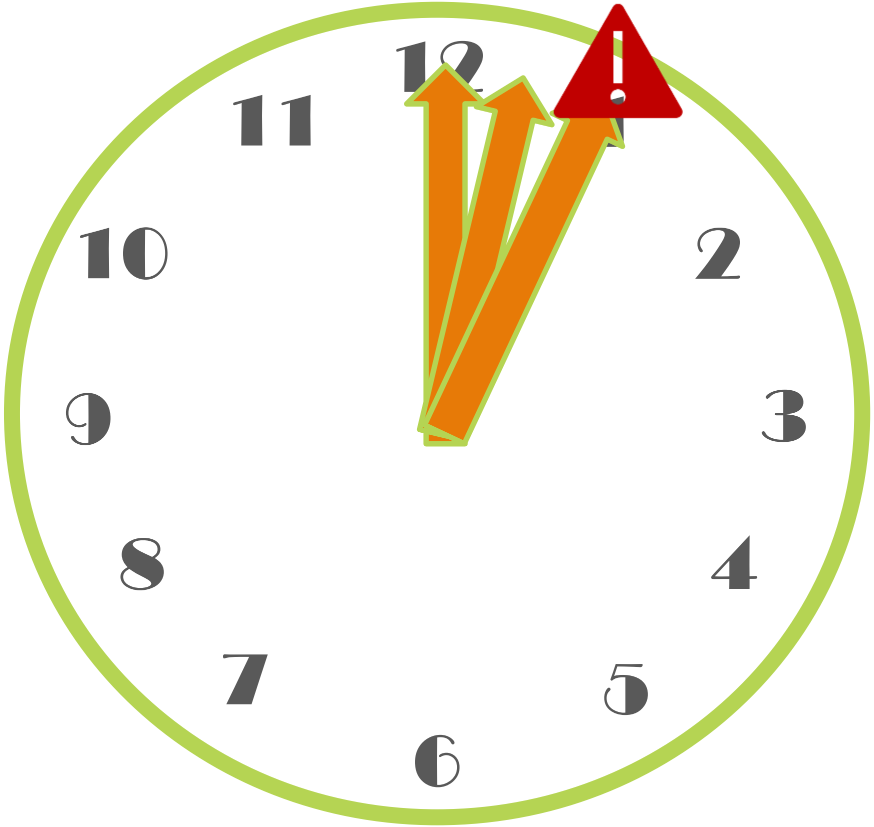
Attackers need to control the endpoint

Attackers objectives require leveraging the endpoint

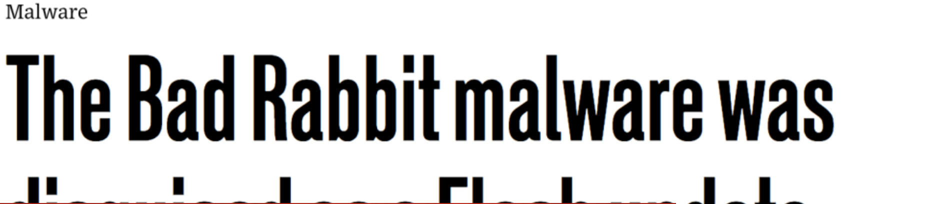


Time to Business Impact of Modern Attacks

- 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



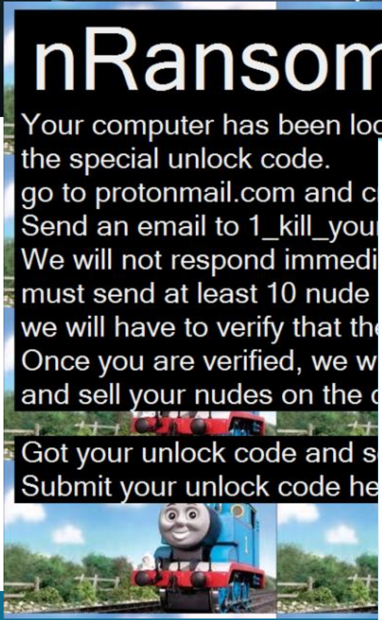
Recent Trend of Ransomware



Malware

The Bad Rabbit malware was disguised as a Flash update

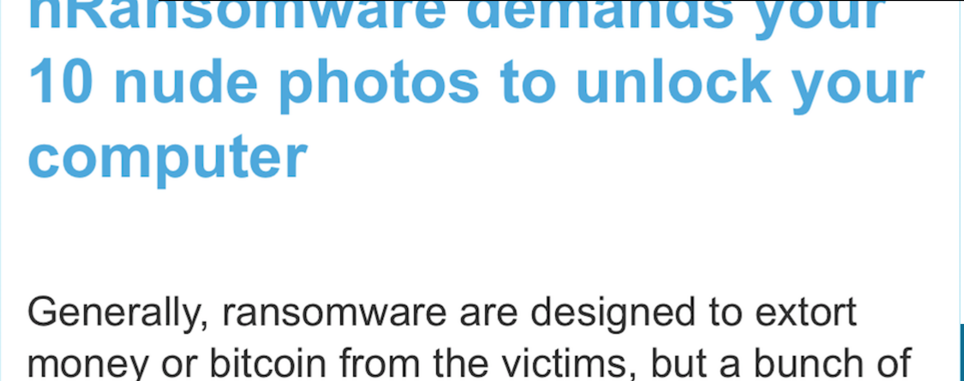
tya but hasn't spread



nRansom

Your computer has been locked. You ca
the special unlock code.
go to protonmail.com and c
Send an email to 1_kill_you
We will not respond immedi
must send at least 10 nude
we will have to verify that the
Once you are verified, we w
and sell your nudes on the d

Got your unlock code and s
Submit your unlock code he

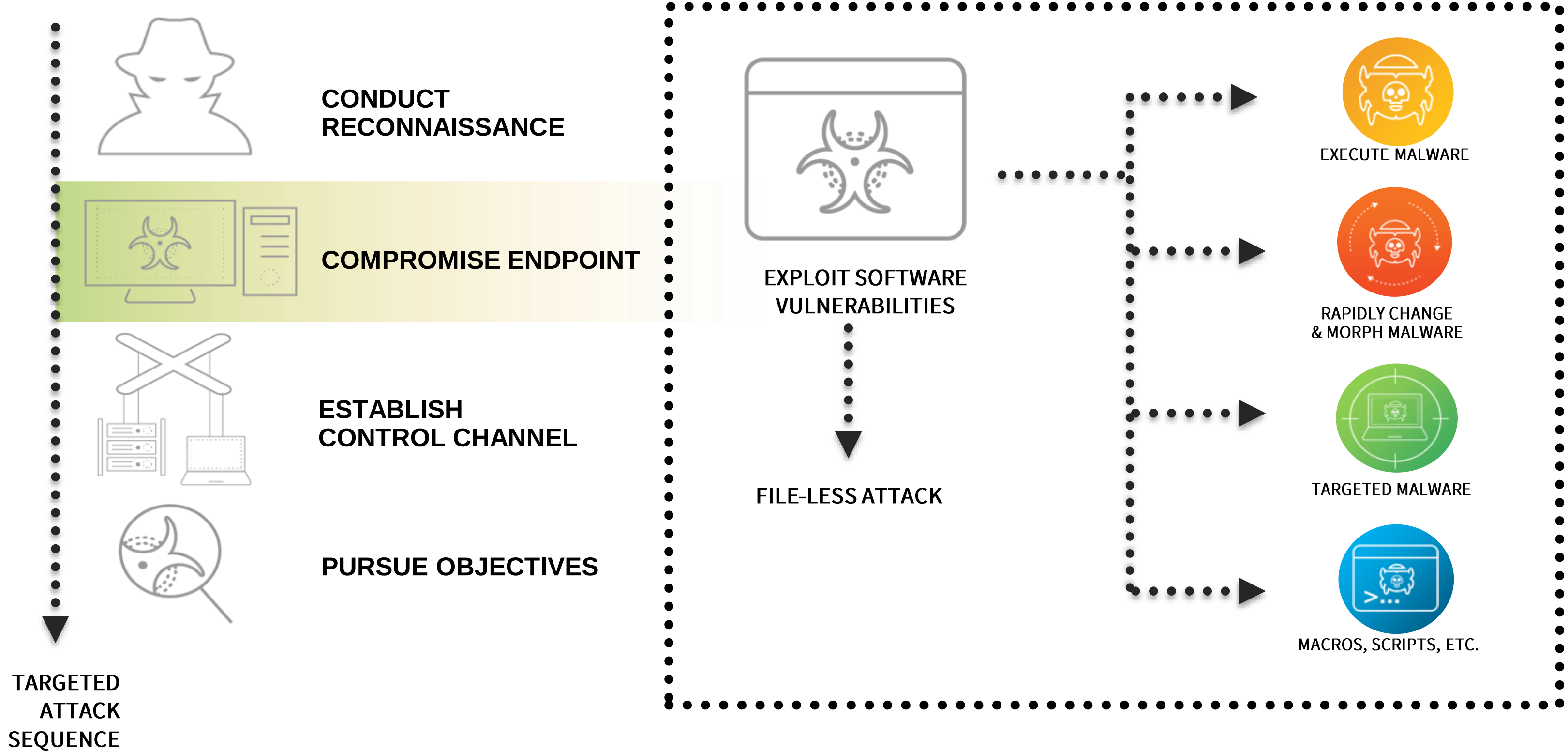


26 Sep

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

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

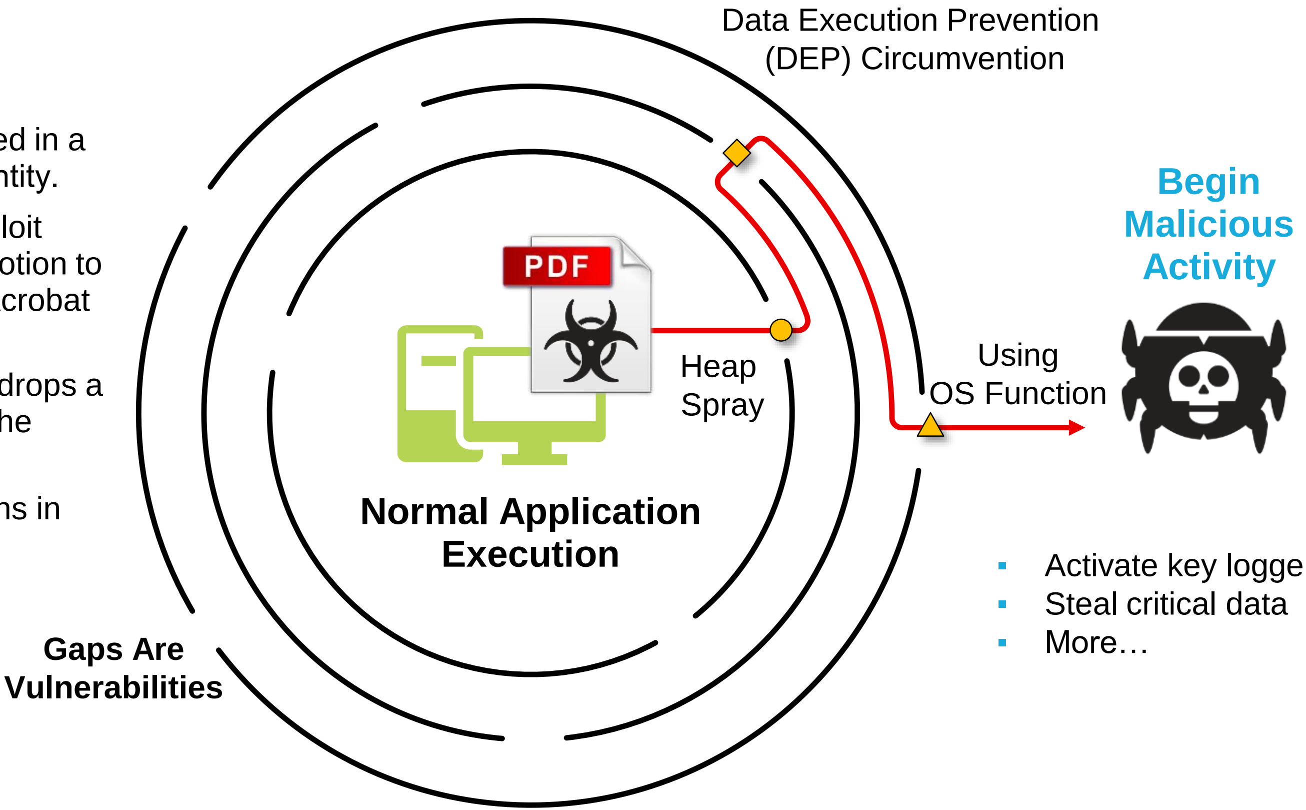
Malware Techniques

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.

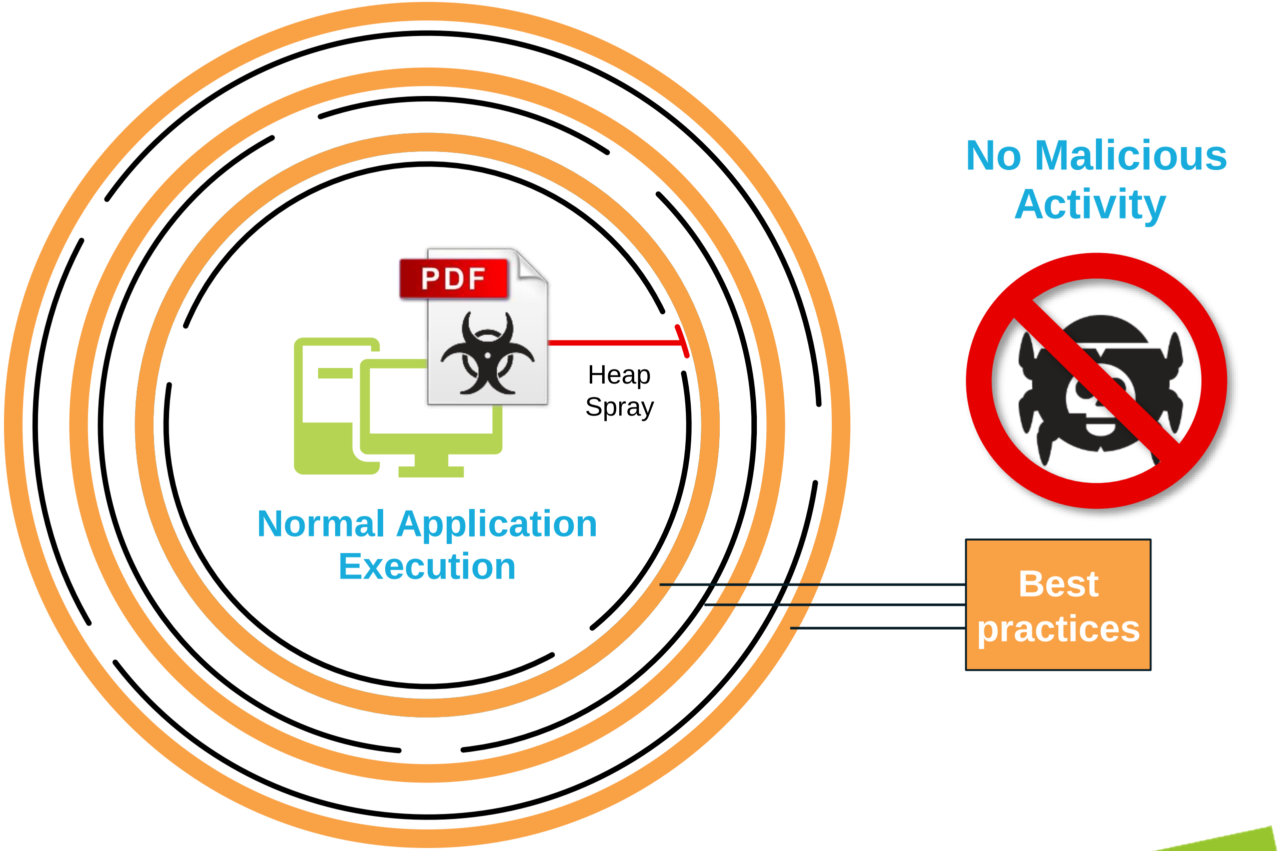


- Activate key logger
- Steal critical data
- More…

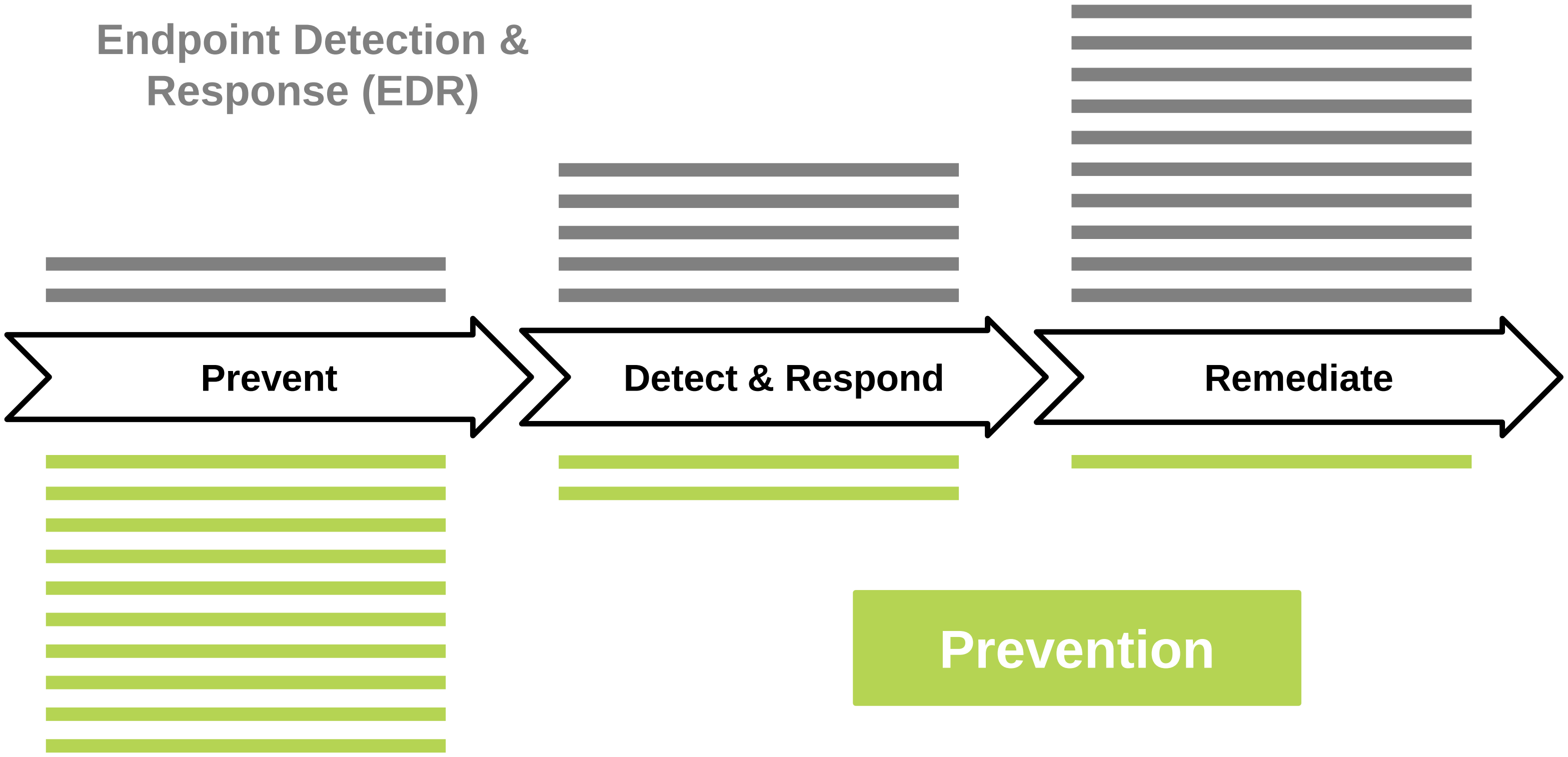
Application Exploit Techniques (Cont.)

Exploit Attack

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



You should be focusing on Prevention



Lower Operating Costs with Accurate, Efficient Alerts

16,937
ALERTS PER WEEK ON AVERAGE
ONLY
4%
CAN BE INVESTIGATED
Ponemon Institute study of 630 enterprises

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 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

Perimeter...

The Cloud...

Hybrid…

Data Center...

Thank You