Successful prevention of ransomware in real life - what can be done in the network and what must be done at the endpoint?

Harri Ruuttila

Systems Engineer

paloalto NETWORKS®

Agenda

- Attack lifecycle
- Examples from the real world
- Best Practices for Threat Protection
- Demo

How does malware get in? Three most common vectors

EXPLOIT KITS OVER WEB

MALICIOUS EMAIL ATTACHMENTS

MALICIOUS LINKS IN EMAILS

WEB: Infected website or malicious ad via exploit kit

STEP 1
User visits compromised website, which is often a trusted location.

STEP 2
Malicious code redirects to exploit kit landing page.
OR
Malicious advertisement silently redirects to malicious web page.

STEP 3
Exploit kit web page loads and determines best route to infect user.

STEP 4
Exploit kit takes advantage of vulnerable software.

STEP 5
Exploit kit delivers malware payload.

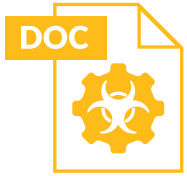
STEP 6
Victim's sensitive files are encrypted and held for ransom. / Attacker has full control of the endpoint.

Top Vulnerabilities Exploited by Drive-by Downloads

EMAIL: Compromised Microsoft Word document

STEP 1
Targeted email with infected Microsoft® Office Word document delivered to user.

STEP 2
User opens Word document, thinking it is a legitimate file.



STEP 3
Office macros run, downloading malware from URLs within the document.

STEP 4
Victim's sensitive files are encrypted and held for ransom. / Attacker has full control of the endpoint.

Targeted and Social Engineering Attacks

- What are the most dangerous file types on the internet today?!

The email contains a link to "PostNord" pages

Kuriren Har Inte levererat Paketet

Vi har fått ditt paket **CT8380159SE** på **2016/01/29**. Courier inte leverera detta paket till dig.

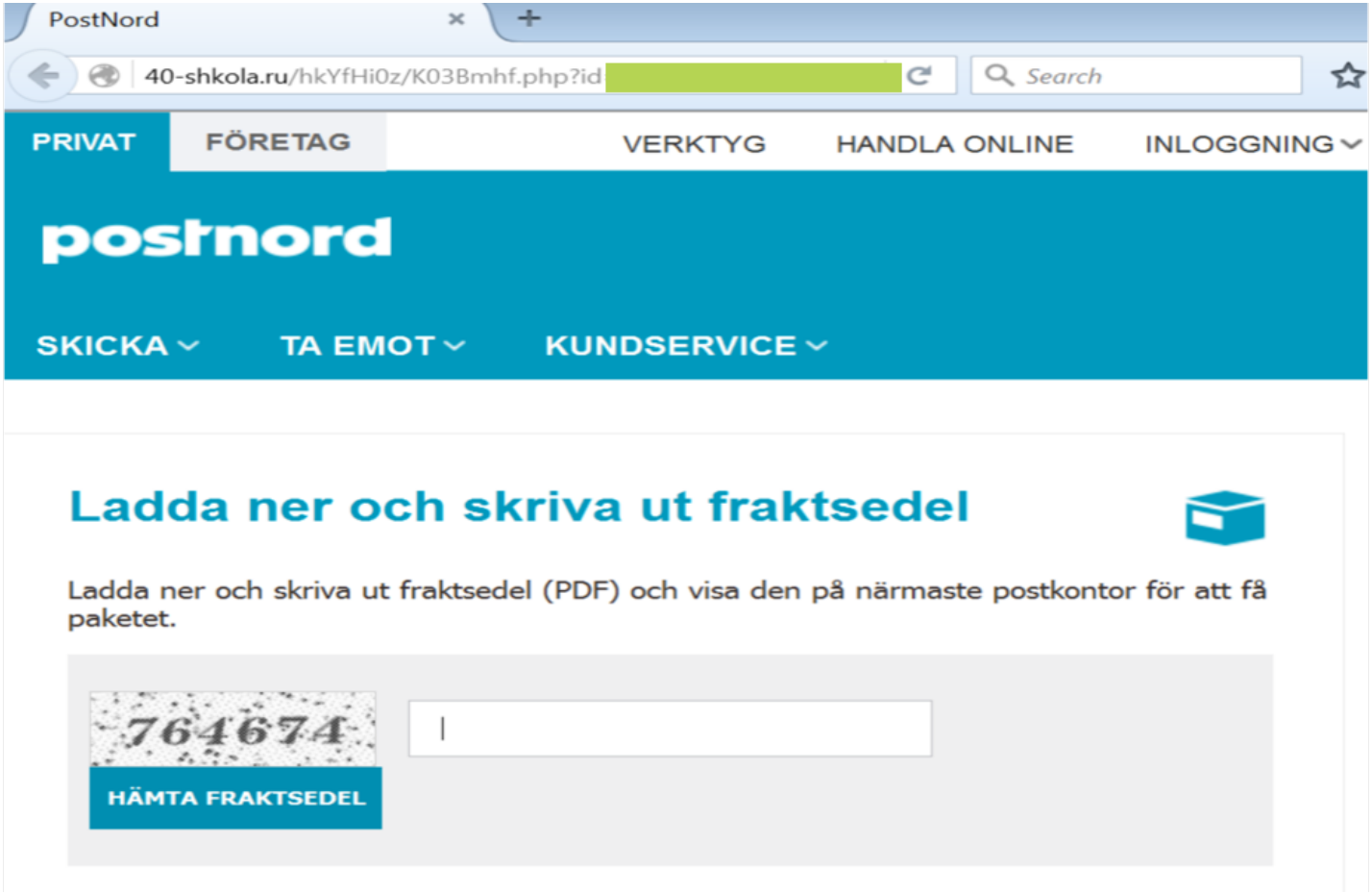
Skriv ut fraktetikett och visa den på närmaste postkontor för att få ditt paket.

Få fraktetikett

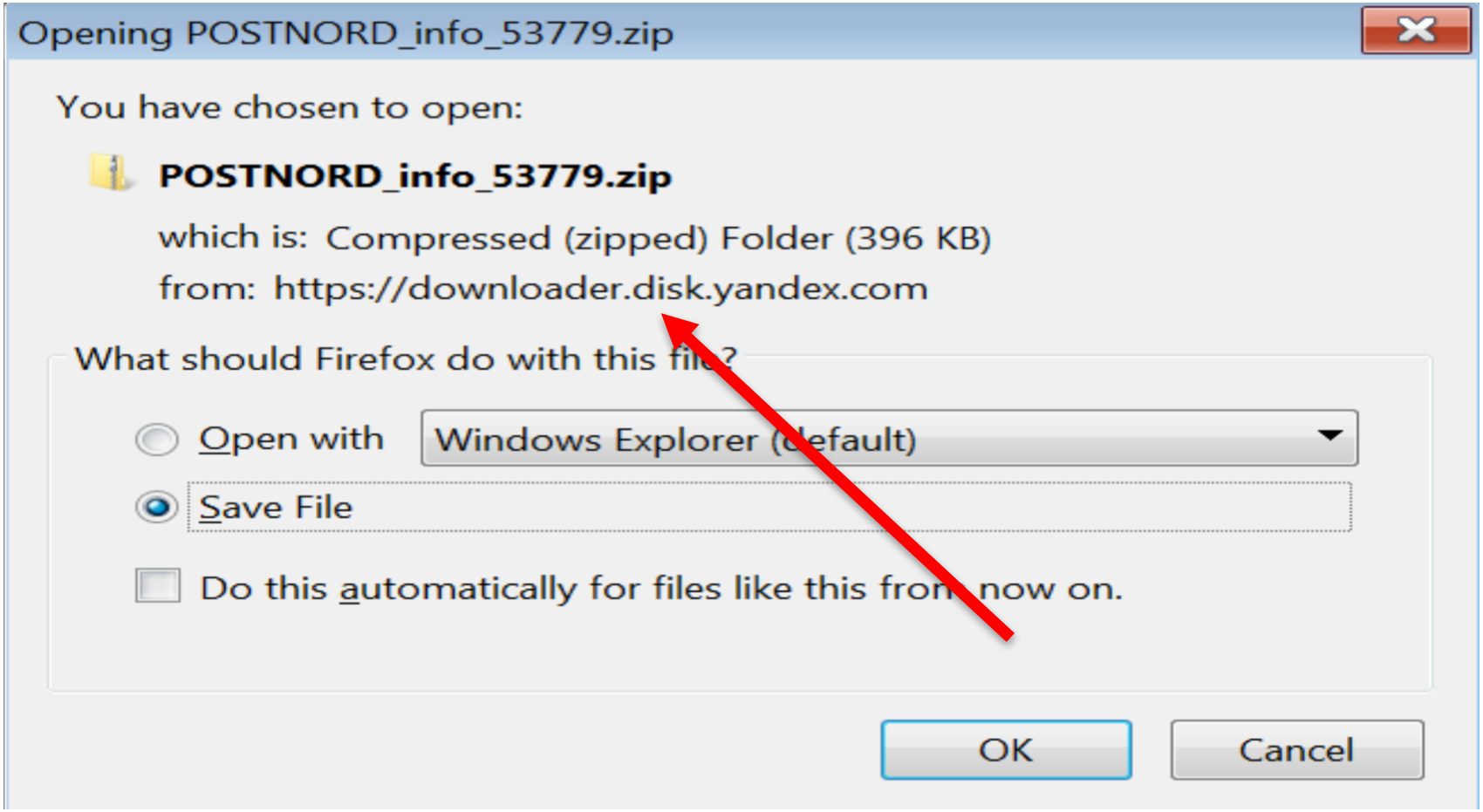
Om paketet inte kommer att tas emot inom 16 arbetsdagar, har Postnord rätt att kräva ersättning från dig - 64 kronor för varje dag för paketet lagring. Du kan hitta information om förfarandet och villkoren för paketet lagring i närmaste kontor.

Detta är ett automatiskt meddelande. Klicka här för att avregistrera.

The link opens a page where a captcha is asked



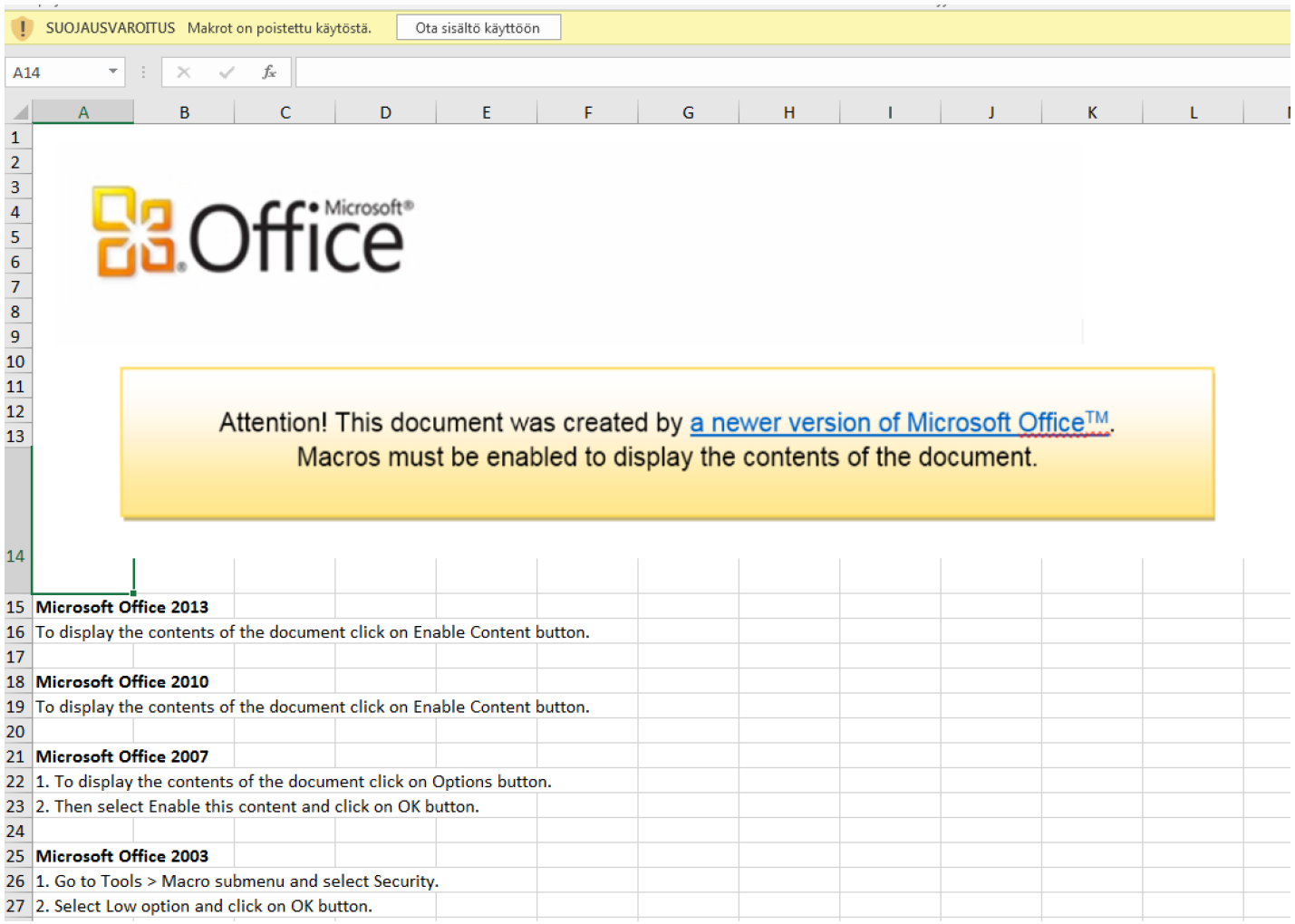
Next a zip file is being downloaded



Zip contains a “pdf” which is actually an application

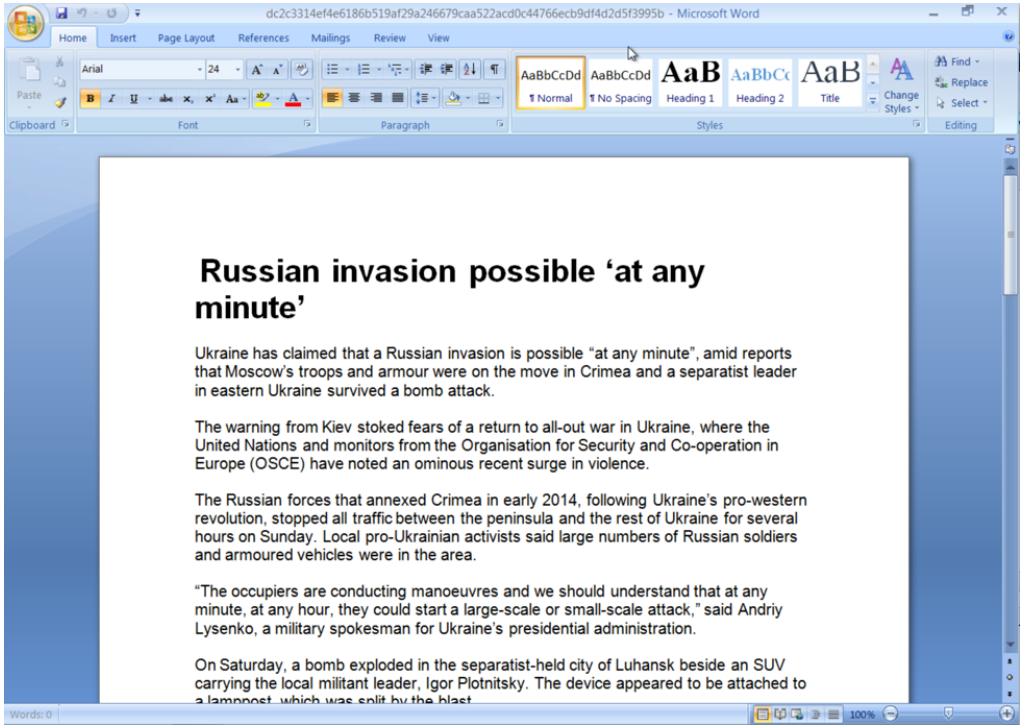
Name	Date modified	Type	Size
POSTNORD_info_53779	2/4/2016 1:38 PM	Application	524 K

Example: Macro based malware downloader



Example: Office document with exploit – Sofacy aka APT28

Decoy document



Russian invasion possible 'at any minute'

Ukraine has claimed that a Russian invasion is possible "at any minute", amid reports that Moscow's troops and armour were on the move in Crimea and a separatist leader in eastern Ukraine survived a bomb attack.

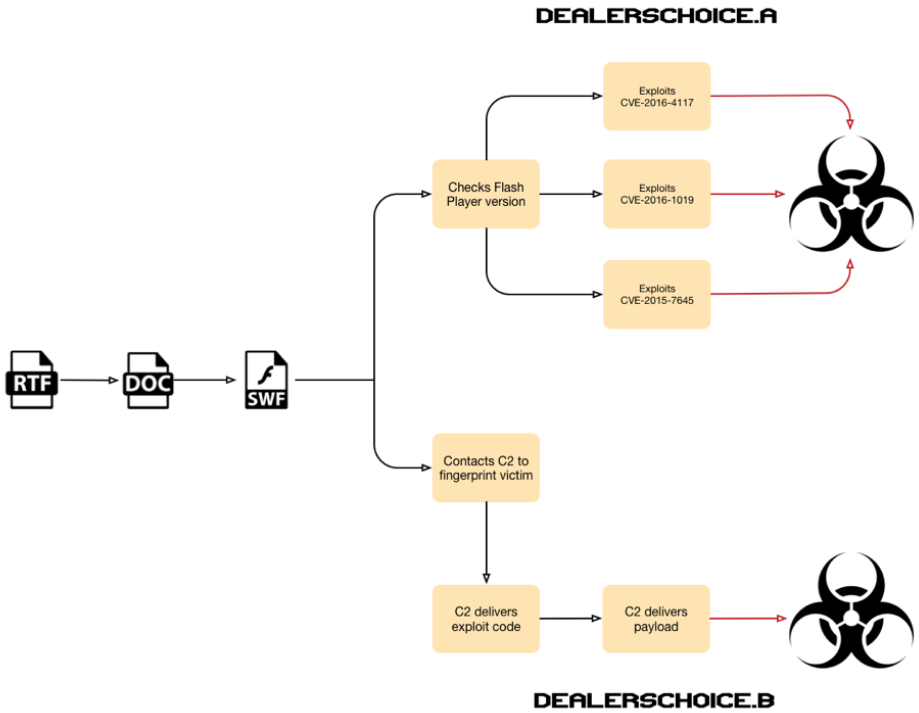
The warning from Kiev stoked fears of a return to all-out war in Ukraine, where the United Nations and monitors from the Organisation for Security and Co-operation in Europe (OSCE) have noted an ominous recent surge in violence.

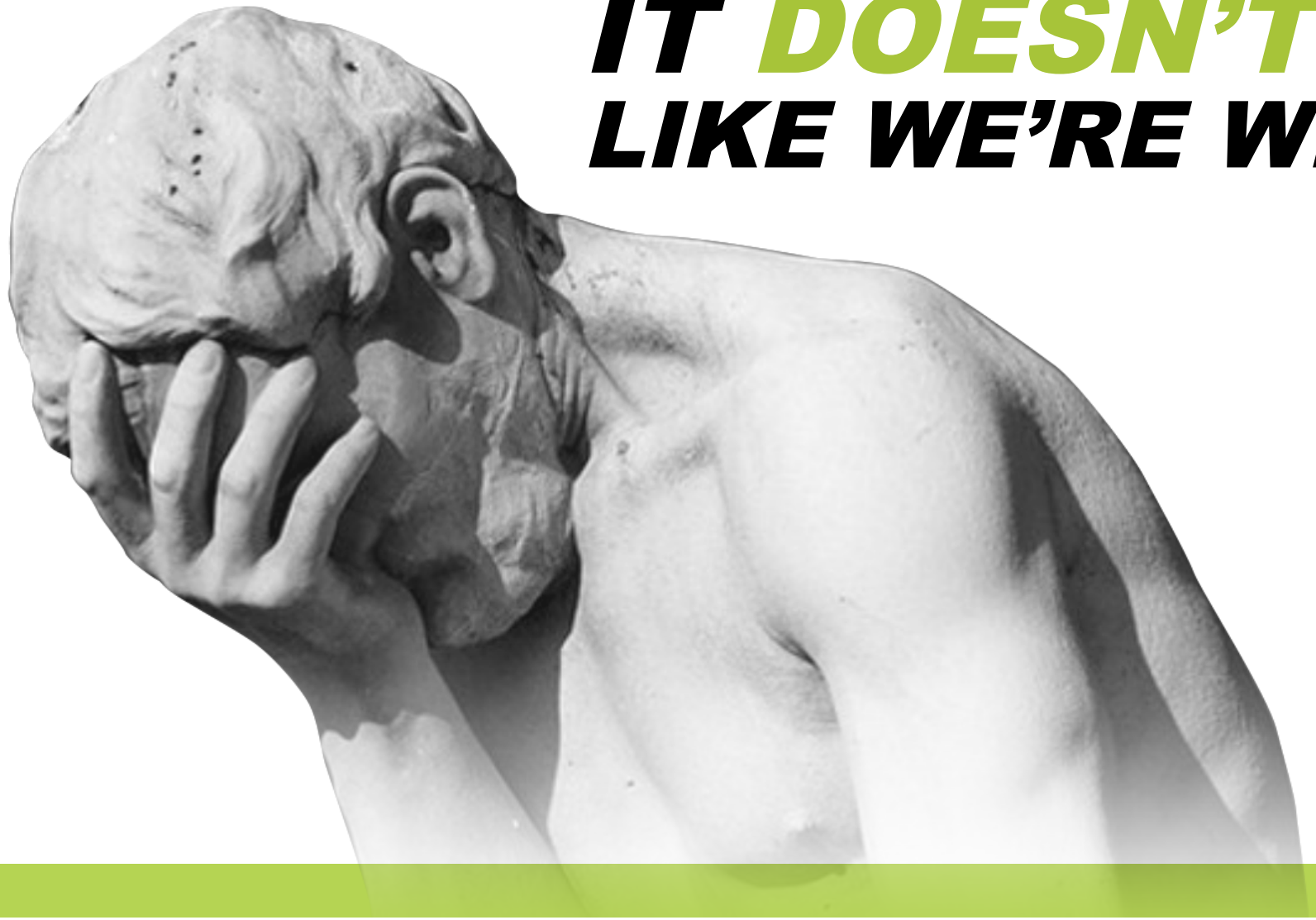
The Russian forces that annexed Crimea in early 2014, following Ukraine's pro-western revolution, stopped all traffic between the peninsula and the rest of Ukraine for several hours on Sunday. Local pro-Ukrainian activists said large numbers of Russian soldiers and armoured vehicles were in the area.

"The occupiers are conducting manoeuvres and we should understand that at any minute, at any hour, they could start a large-scale or small-scale attack," said Andriy Lysenko, a military spokesman for Ukraine's presidential administration.

On Saturday, a bomb exploded in the separatist-held city of Luhansk beside an SUV carrying the local militant leader, Igor Plotnitsky. The device appeared to be attached to

Exploits





IT DOESN'T FEEL LIKE WE'RE WINNING

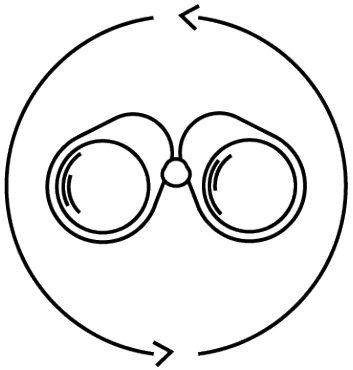
paloalto NETWORKS®

PREVENTION 1ST

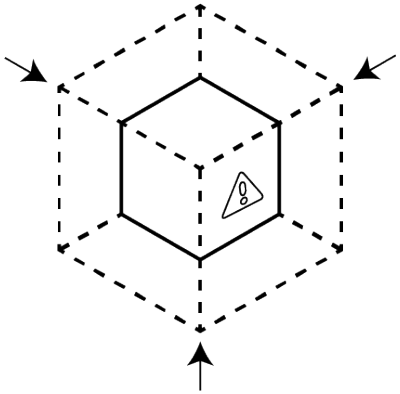
Leveraging the Entire Network Security Platform

Top tips to stop ransomware / malware / breaches

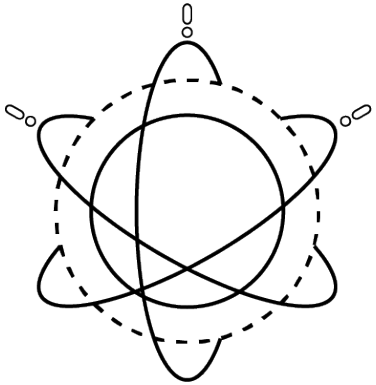
Prevention imperatives



COMPLETE VISIBILITY



REDUCE ATTACK SURFACE



PREVENT KNOWN THREATS

PREVENT UNKNOWN THREATS

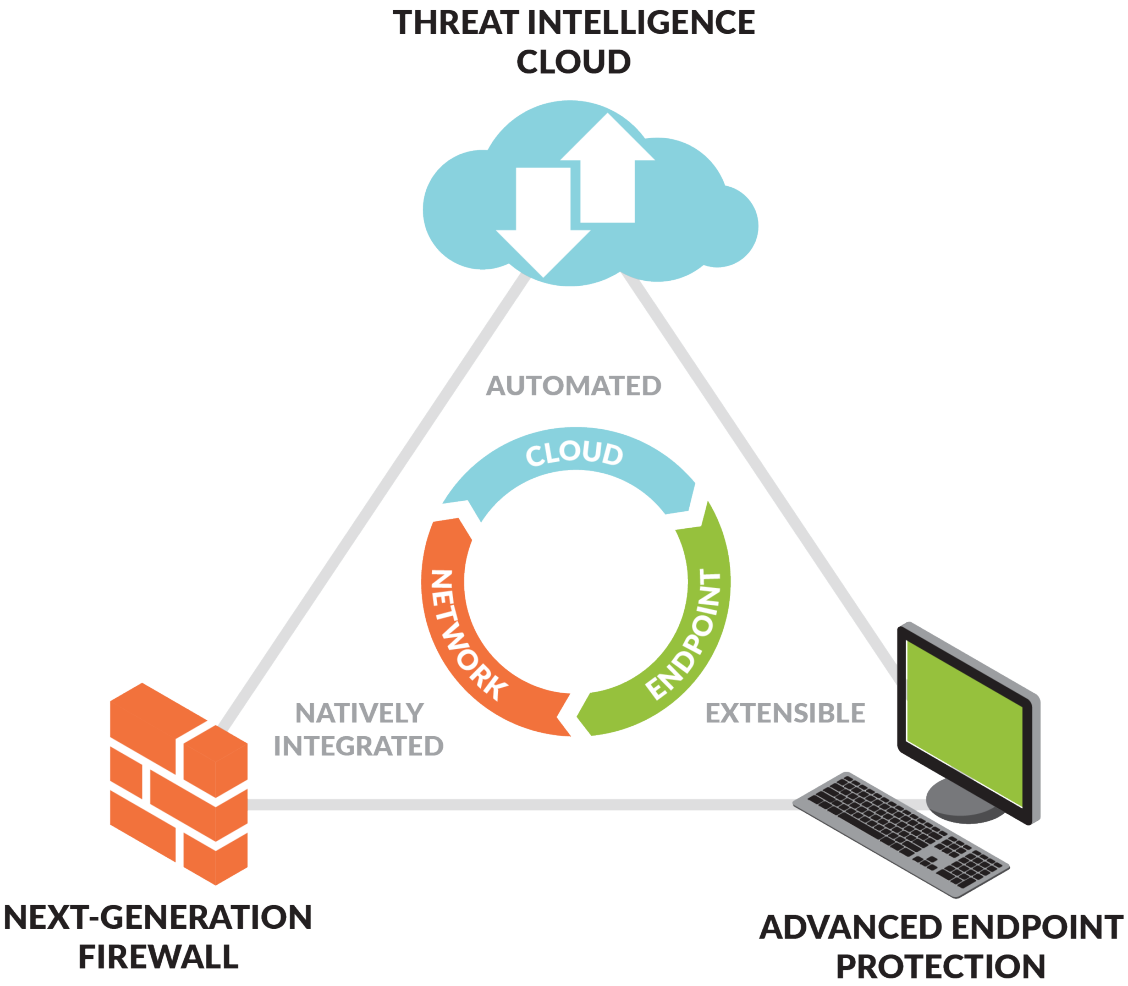
Prevention imperatives

Complete visibility	Reduce attack surface area	Prevent all known threats	Prevent new threats
• All applications • All users • All content • Encrypted traffic	• Enable business apps • Block “bad” apps • Limit app functions • Limit file types • Block websites	• Exploits • Malware • C&C • Malicious websites • Bad domains • Stolen credentials	• Dynamic analysis • Static analysis • Attack techniques • Anomaly detection • Analytics

Prevention imperatives

Complete visibility	Reduce attack surface area	Prevent all known threats	Prevent new threats
• All applications • All users • All content • Encrypted traffic	• Enable business apps • Block "bad" apps • Limit app functions • Limit file types • Block websites	• Exploits • Malware • C&C • Malicious websites • Bad domains • Stolen credentials	• Dynamic analysis • Static analysis • Attack techniques • Anomaly detection • Analytics
• Firewall • NAC • Proxy • VPN • SSL decryptor • Endpoint detection	• Firewall • CASB • IPS • Proxy • URL Filter	• IPS • Antivirus • URL filter • 2-factor auth • Anti-spyware • Endpoint security	• Network sandbox • Endpoint sandbox • Machine learning • Big data

Delivering the next-generation security platform



1. Network level controls to block ransomware / malware

- Prerequisite: a true NGFW capable of matching traffic per application not per port. -> Enables granular control to applications based on their risk not the port.

UTM - “NGFW”

Block / **Allow**
Yes Upload and Yes Download
All employees

All allowed applications on the same port have the same security profile.

Block / **Allow**
Yes Upload and Yes Download
All employees

Your collaboration tool

box

SSL
AV
Spyware
IPS
Unknowns

Dropbox

Your partner’s collaboration tool

True next generation

Allow
Yes Upload and Yes Download
All employees

Treat every application based on their risk

Allow
No Upload but Yes Download
Only Legal Dpt. John, Lisa & Joe

22 | © 2015, Palo Alto Networks. Confidential and Proprietary.

2. Network level controls to block ransomware / malware

- Whitelist business required applications -> all unknown and risky applications are denied by default. Bring back the default deny action on firewall.
- Reduce your attack surface by controlling the application actions and file types traversing the network
  - As seen in the example before. Control how applications can be used.
  - Block all PE files (.EXE, .CPL, .DLL, .OCX, .SYS, .SCR, .DRV, .EFI, .FON, .PIF) from suspicious categories (Unknown, dynamic DNS etc.)
  - Block: .HLP, and .LNK files
  - Block .CHM, .BAT and .VBS files
  - Block or Alert on encrypted file types (.zip and .rar) – consider an indicator
  - Alert on all other file types for visibility in both direction

3. Network level controls to block ransomware / malware

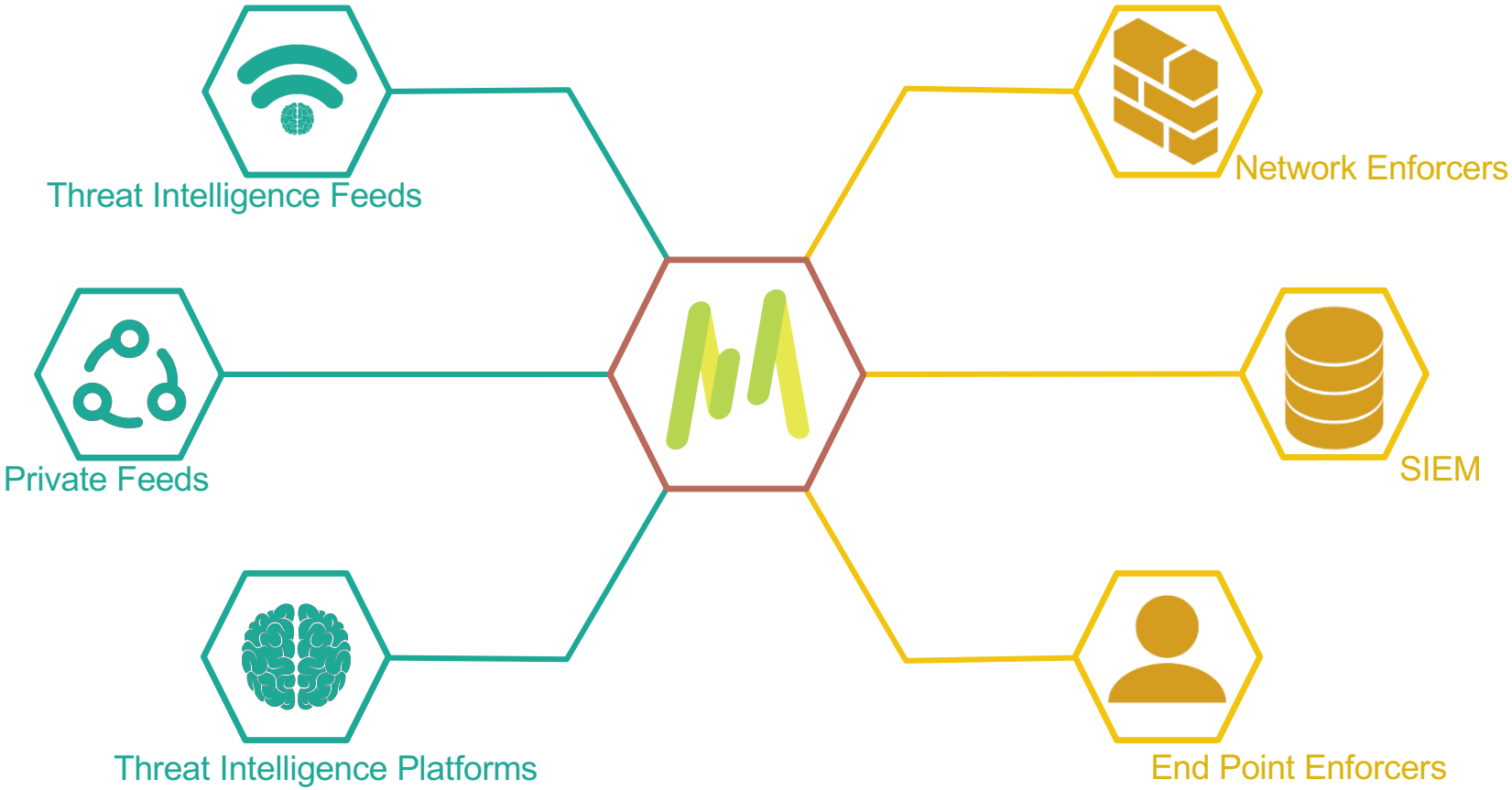
- Reduce attack surface with URL filtering
- Examples of potentially Dangerous Places on the web:
  - Malware categorized websites - BLOCK
  - Phishing websites - BLOCK
  - Dynamic DNS domains used by Remote Access Trojans and malware – BLOCK / CONTINUE and block PE files
  - Unknown domains – ALLOW/CONTINUE and block PE files
  - Parked domains – BLOCK / CONTINUE
  - Questionable category domains BLOCK/CONTINUE and block PE files
  - Proxy-Avoidance BLOCK

4. Network level controls to block ransomware / malware

- Reduce attack surface with External dynamic lists
- Aggregate external threat intel into Palo Alto Networks firewall policy
  - Automatically pull in IP addresses and domains and take action in policy (not just block)
- Possible 3rd party Sources Included on AppSpot site:
  - http://panwdbl.appspot.com/

5. Network level controls to block ransomware / malware

- Intoducing MineMeld - An extensible TI processing framework



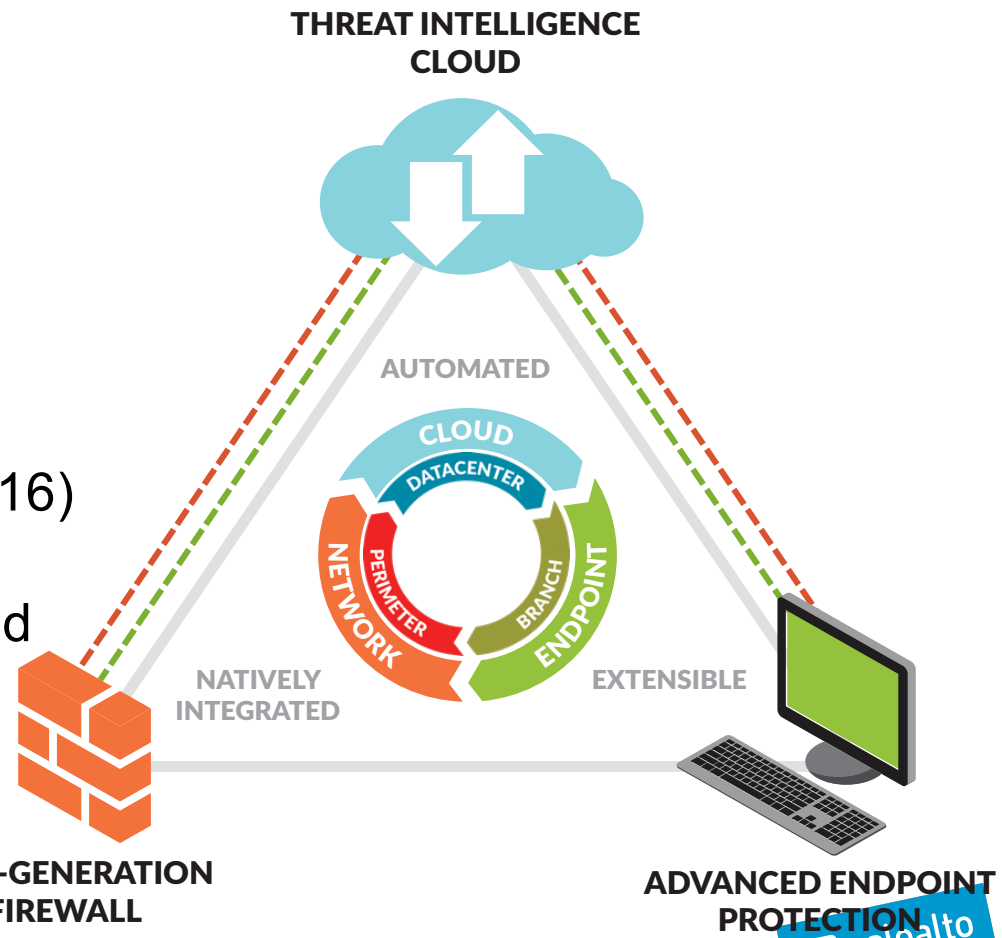
https://live.paloaltonetworks.com/t5/MineMeld/ct-p/MineMeld

6. Network level controls to block ransomware / malware

- Prevent the known badness
- URL Filtering enabled on all ports and applications.
  - Utilize URL categories in policy.
- IPS enabled with all signatures to all applications on all ports (on all rules in the policy)
- AV enabled with all signatures to all applications on all ports (on all rules in the policy)
- AntiSpyware enabled with all signatures to all applications on all ports (on all rules in the policy)
- No need to “tune” signature set for performance -> True Single Pass NGFW

7. Network level controls to block ransomware / malware

- Sandbox all unknown files per policy
- Available in US, EU and locally
- > 1,000,000 remote sensors
- Largest Threat database (Forrester 2016)
- Any unknown into a known in 5 min and
- All FWs and Endpoints reprogrammed automatically



Is this enough?

Network controls can only protect what they can see…

- SSL/TLS
  - If you are not decrypting SSL/TLS traffic, you are blind at the network level for attacks arriving on encrypted streams.
  - Some applications cannot be decrypted. (certificate pinning, client cert auth etc.)
- Emails in the cloud
  - Malware arrives at the end user mailbox in the cloud and is downloaded via encrypted stream to the endpoint.
- Classic USB-stick vector or similar
  - Network cannot see what does not traverse over it.
    - 2016 Blackhat USA: “48 percent of USB drives were picked up and plugged into a computer with the user clicking on files.”
- Network level obfuscation / custom encryption etc..
- You need to take the fight to the endpoint.

Main ways to infect an endpoint

Exploits

Weaponized Data Files & Content

Subvert Normal Applications

≠

Malware

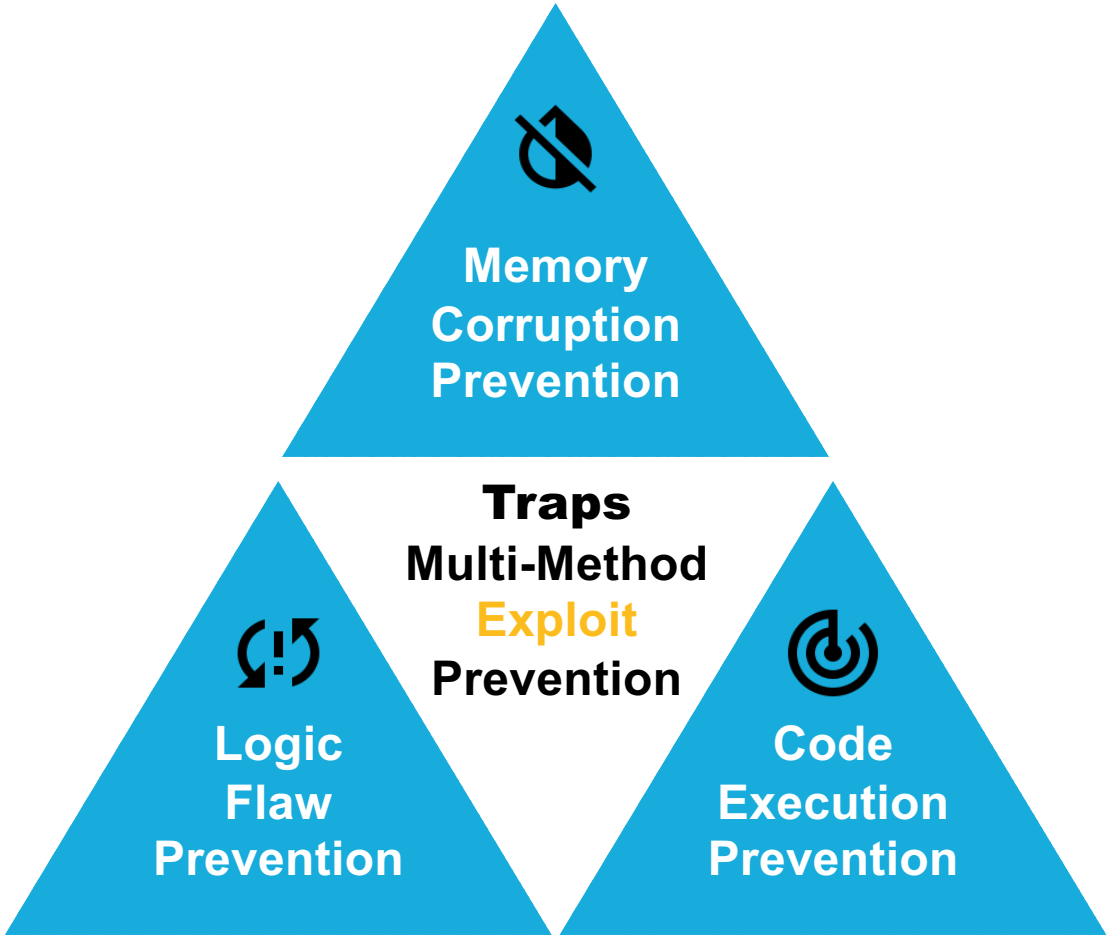
Executable Programs

Carry Out Malicious Activity

8. Endpoint level controls to block ransomware / malware

- Block all exploits.
  - Known – the easy part
  - Unknown 0-day exploits – the hard part

- How?
  - By focusing on the building blocks of exploits not individual vulnerabilities nor exploits.

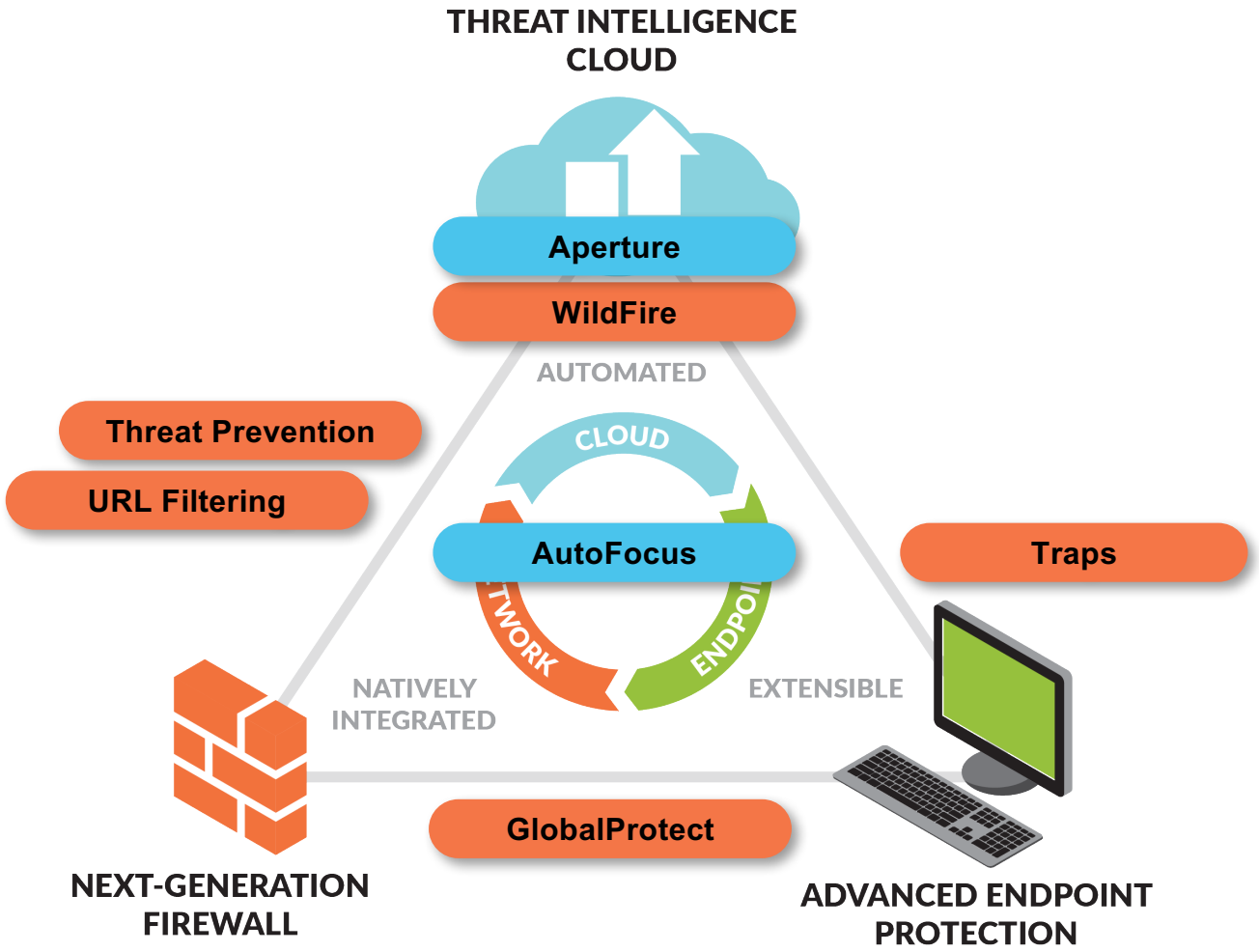


9. Endpoint level controls to block ransomware / malware

- Block all malware.
  - Known – the easy part
  - Unknown – the hard part
- Reduce attack surface on the endpoint
  - Restrictions
  - Behavioral protections
- How?
  - Using multiple methods with multiple purpose build techniques.

What next?

Delivering the next-generation security platform



Traps Demo

1. Malware prevention
    1. Wildfire known sample
    2. Local Analysis sample
    3. Restrictions (Child process)
2. Exploit prevention
    1. Browser based Flash exploits
    2. Office document Flash exploit
        Sofacy aka APT28