Leveraging the cyber kill chain in your favor

how to tear down modern Malware or latest in Targeted Attacks

Kilian Zantop

SE Switzerland

paloalto NETWORKS

Definition

- **Malware**, short for **malicious software**, is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems.[1] It can appear in the form of code, scripts, active content, and other software.[2] 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software

- **Advanced persistent threat** (**APT**) usually refers to a group, such as a government, with both the capability and the intent to persistently and effectively target a specific entity. The term is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage using a variety of intelligence gathering techniques to access sensitive information,[1] but applies equally to other threats such as that of traditional espionage or attack.[2] Other recognized attack vectors include infected media, supply chain compromise, and social engineering. Individuals, such as an individual hacker, are not usually referred to as an APT as they rarely have the resources to be both advanced and persistent even if they are intent on gaining access to, or attacking, a specific target.

www.wikipedia.org

The bad news

- A New Threat Landscape
- The dark side has improved to professional standards

A New Threat Landscape

Nordkorea rüstet auf für den Krieg im Internet!

Diktator Kim Jong-un befehligt mittlerweile 6000 Hacker in seiner Sondereinheit „Büro 121“. Doppelt so viele wie bisher angenommen!

Die neuen Zahlen stammen aus einer Analys
Verteidigungsministeriums.

Kims Sondereinheit „Büro 121" besteht aus 6000 Hack
Armeeeinheit einen Computerbildschirm. Was darauf z

Foto: dpa

Fastest growing

Anonymous: bundeskanzlerin.de down

bundestag.de,

07.01.2015

www.bundeskanzlerin.de und www.bundestag.de down. Seit einer Stunde sind die Seiten offline, nicht mal anpingbar. Es kommt die Fehlermeldung "Server nicht gefunden". Die Hintergründe sind unklar. Eine offizielle Begründung gibt es nicht. Hat die Regierung etwa ihre Domaingebühren nicht bezahlt oder wurde die Seite gehackt?

Fakt ist, dass die Seite nicht erreichbar ist - aus welchen Gründen auch immer. So richtig vermisst wird die Seite jedoch kaum. Denn was die Blockparteien dort zu sagen haben, ist sowieso meist das Gleiche und ändern wird sich auch nichts...

Update: Anonymous steckt wohl dahinter:

Merkel Tango Down: Wir haben diese verkommene Bundesregierung gewarnt. Diese verkommene Bundesregierung wollte nicht hören. Cyberberkut und Anonymous haben www.bundeskanzlerin.de und www.bundestag.de vom Netz genommen. Wir sind Anonymous. Wir sind viele. Wir vergeben nicht. Wir vergessen nicht. Erwartet uns. #FreeUkraine

The dark side has improved to professional standards

- Criminal orgnisation
  - Have very good founding
  - Hire professionals
  - Attack financialy interesting targets
- Goverments
  - Have limitless resources and budget
  - Get all the specialists they want
  - No need to for profit
- Political groups
  - Are usually extremists and radical
  - Are fanatics and nothing to loose
  - No need to gain profits

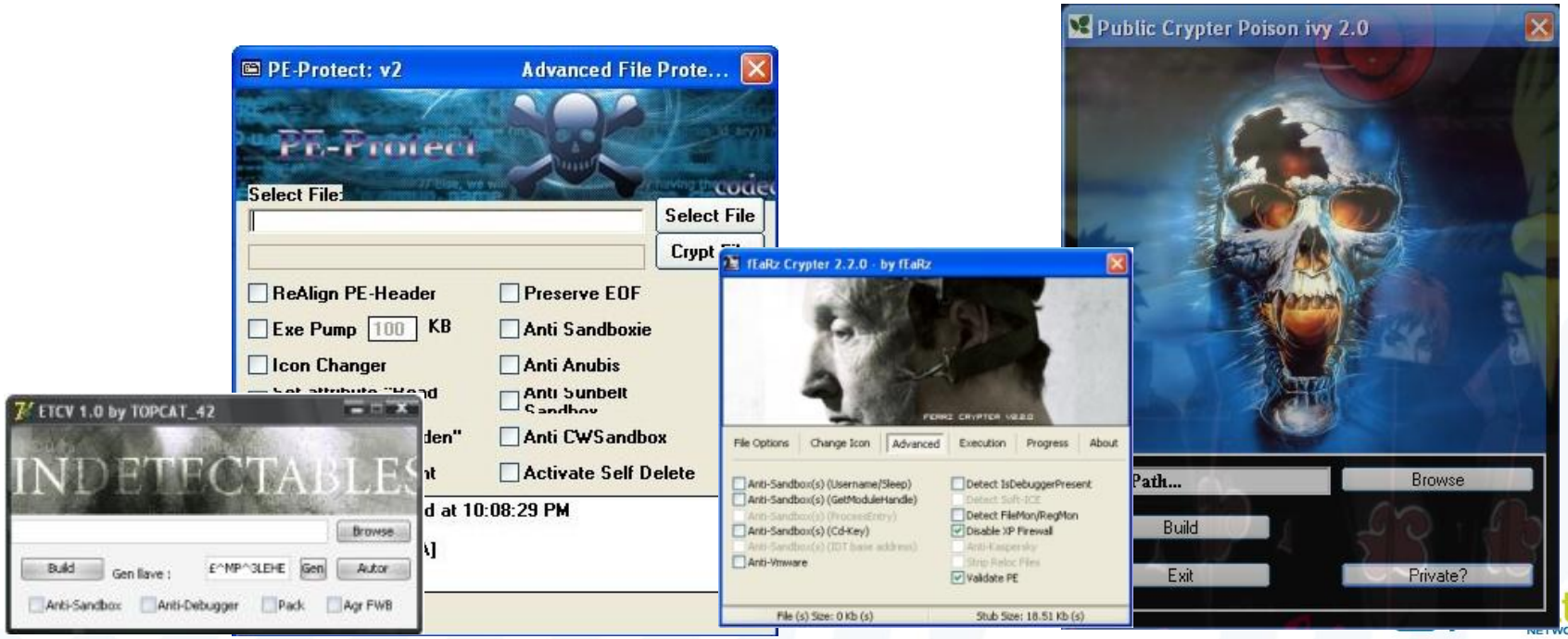
The dark side has improved to professional standards

- Cybercriminals developed formidable tools

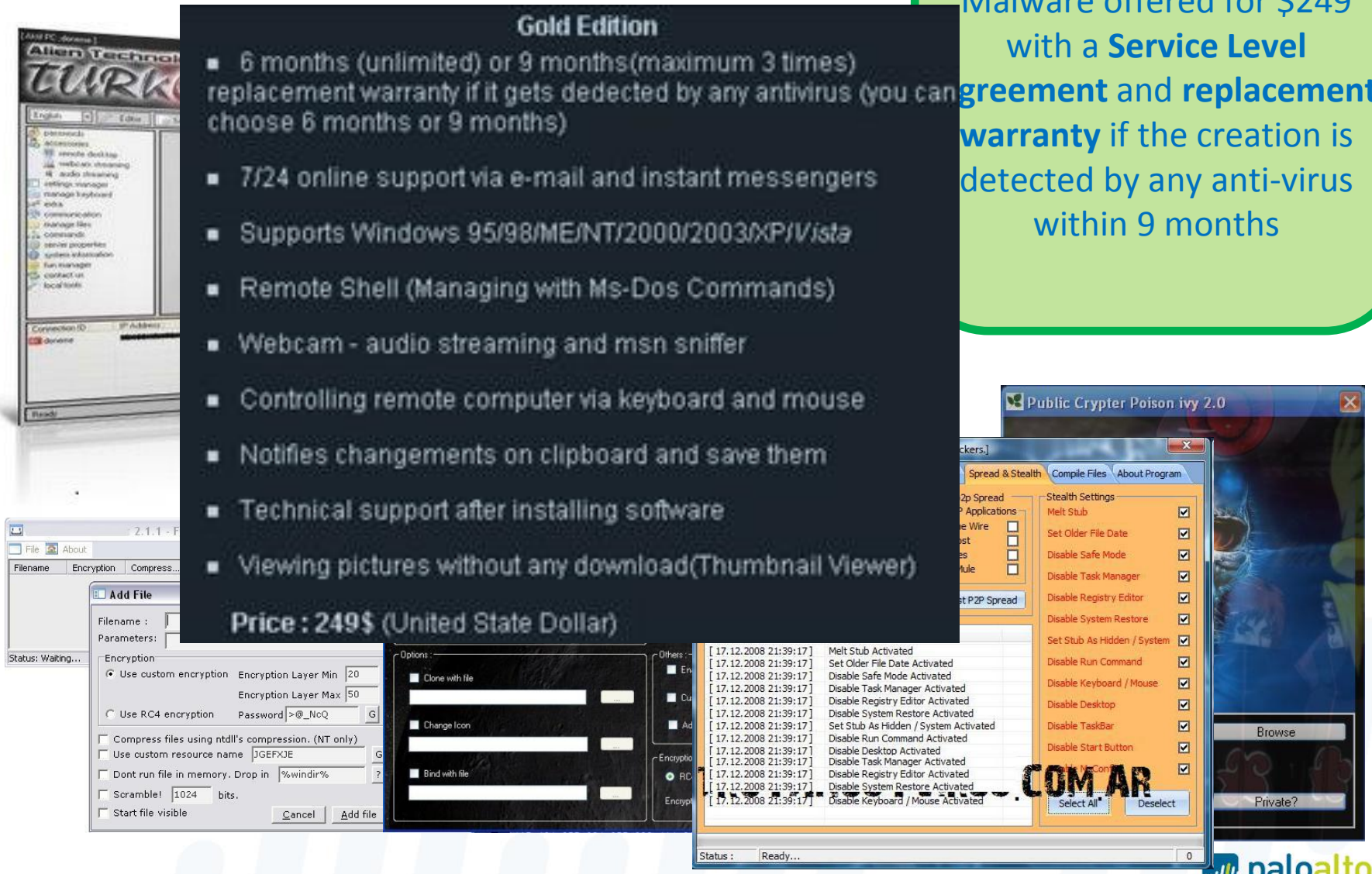
Easy to use development tools, Q&A, and service level agreements just as in every mature industry

- Detection Evasion and Resilience

By design, malware is developed and deployed with detection evasion in mind



Malware offered for $249 with a **Service Level greement** and **replacement warranty** if the creation is detected by any anti-virus within 9 months



The dark side has improved to professional standards

Credit Card : 67669

BIN	BRAND	LEVEL	M	Y	COUNTRY	ZIP	PHONE	PRICE	BANK	DOB	ADRESS
379725	AMERICAN EXPRESS		8	2016	US			8 $	AMERICAN EXPRESS US		
379727	AMERICAN EXPRESS		9	2016	US			8 $	AMERICAN EXPRESS US		
379731	AMERICAN EXPRESS		12	2016	US			8 $	AMERICAN EXPRESS US		
379732	AMERICAN EXPRESS		12	2016	US			8 $	AMERICAN EXPRESS US		
371101	AMERICAN EXPRESS		3	2015	US			4 $	AMERICAN EXPRESS COMPANY		
371240	AMERICAN EXPRESS	GREEN	12	2016	US			4 $	AMERICAN EXPRESS COMPANY		

SHELL	NEW HACKED	UPLOAD/UNZIP WORKS	******	******	3.50	Buy
SHELL	NEW HACKED	UPLOAD/UNZIP WORKS	******	******	3.50	Buy
SHELL	NEW HACKED	UPLOAD/UNZIP WORKS	******	******	3.50	Buy
	USA-2008	Arizona (AZ)	WIN 2008	Ia****	******	7.00

paloalto NETWORKS

Available to amteurs as well ..

The number of retailgrade tools increases ..

More bad news

- The mass and the speed of new malware
- Not the sophistication of the single tool

Threat Highlight: Kuluoz

One particular malware family, Kuluoz (also known as Asprox), stood out as exceptionally prevalent in the sample data. This single family accounts for 4.9 million malicious sessions recorded during the month of October 2014, with 1,933 companies across all 10 industries impacted. WildFire identified a total of 268,084 unique samples determined to be Kuluoz, 82.4% of which had not been collected by VirusTotal at the time of analysis.

KULUOZ STATISTICS	
% of Companies Impacted	81.8
% of Malicious Sessions	80.0
% of Unique Malware	74.4

By 2013, the primary components of Asprox had been replaced by a new malware family dubbed Kuluoz. While Asprox was an “all-in-one” malware, Kuluoz uses a modular design, which allows it to evade detection and gives attackers more flexibility. In May we identified a new campaign distributing Kuluoz that was generating over 30,000 new WildFire sessions per hour. Since that time Kuluoz has persisted to be highly prevalent across the entire world and the October data shows this pattern continues.

Threat Highlight: Kuluoz

E-mail themes for Kuluoz propagation spam have varied greatly and normally come in waves. These include legal notices (e.g., court order), package delivery messages (e.g., FedEx, UPS, DHL), voicemail service notifications (e.g., WhatsApp), current events (e.g., 2014 polar vortex), and online deals (e.g., free pizza from Pizza Hut), to name just a few.

A very similar pattern is apparent in the total number of unique Kuluoz samples detected throughout the month. The Kuluoz attackers stay ahead of antivirus detection by regularly regenerating the malware so that it frequently appears brand new, despite containing the same functionality.

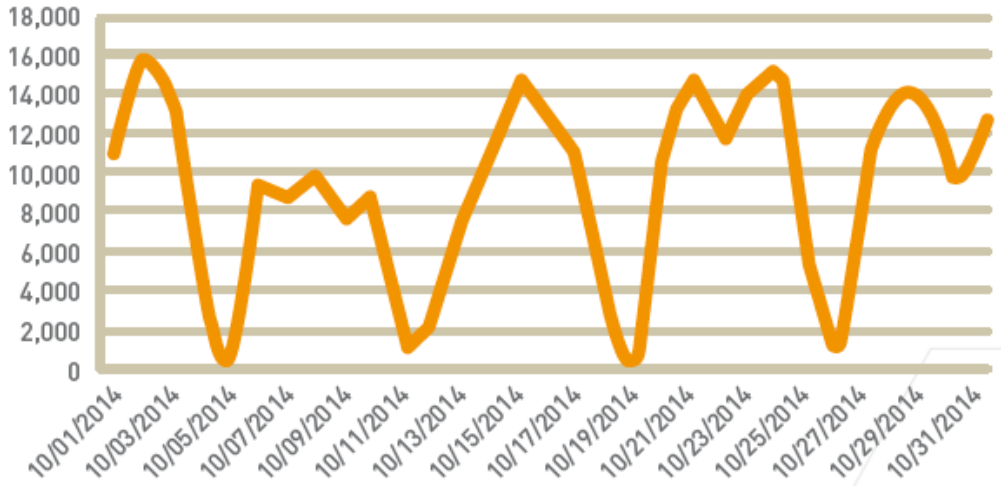


Figure 47: WildFire Kuluoz Detections (Unique Samples by Day)

Statistics: Number of vulnerabilities

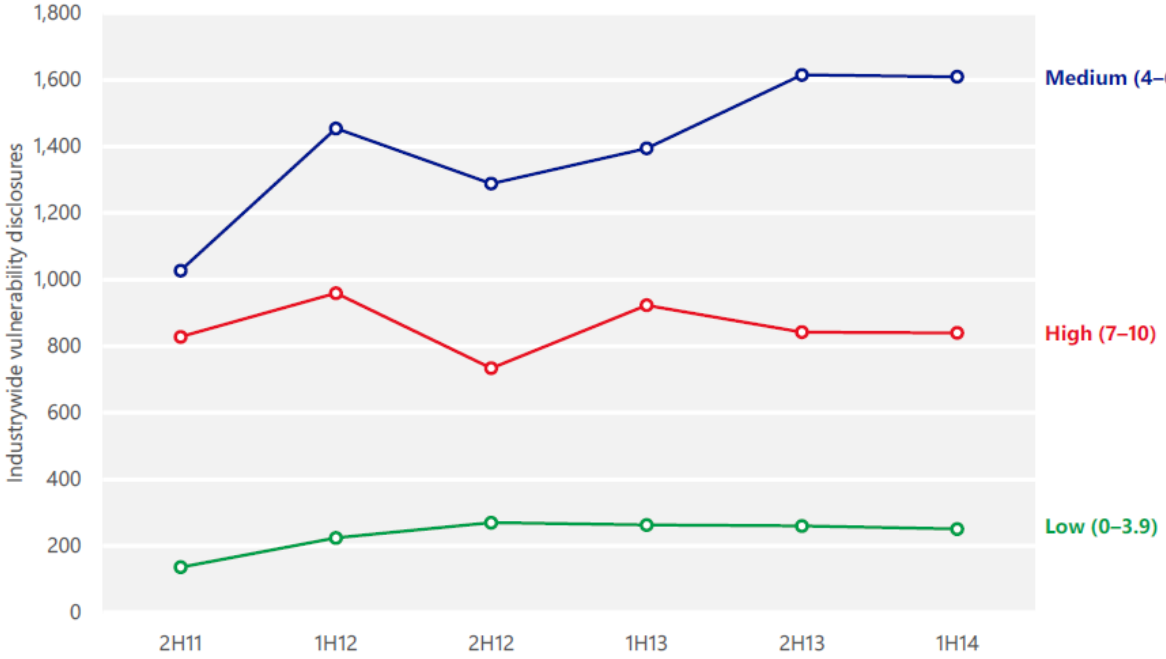
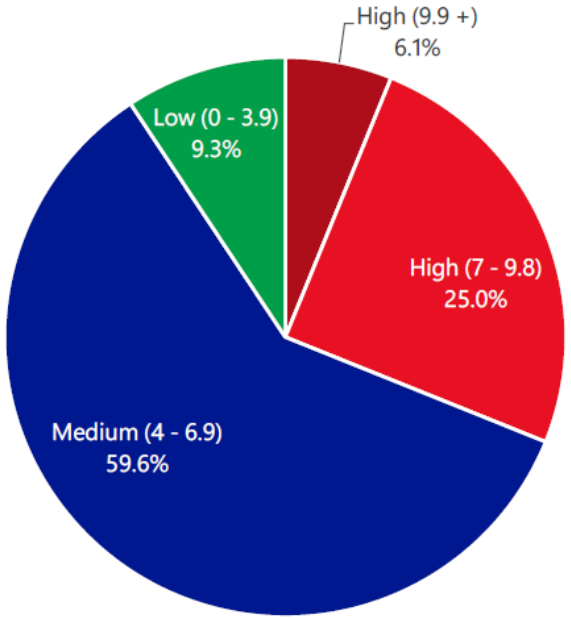


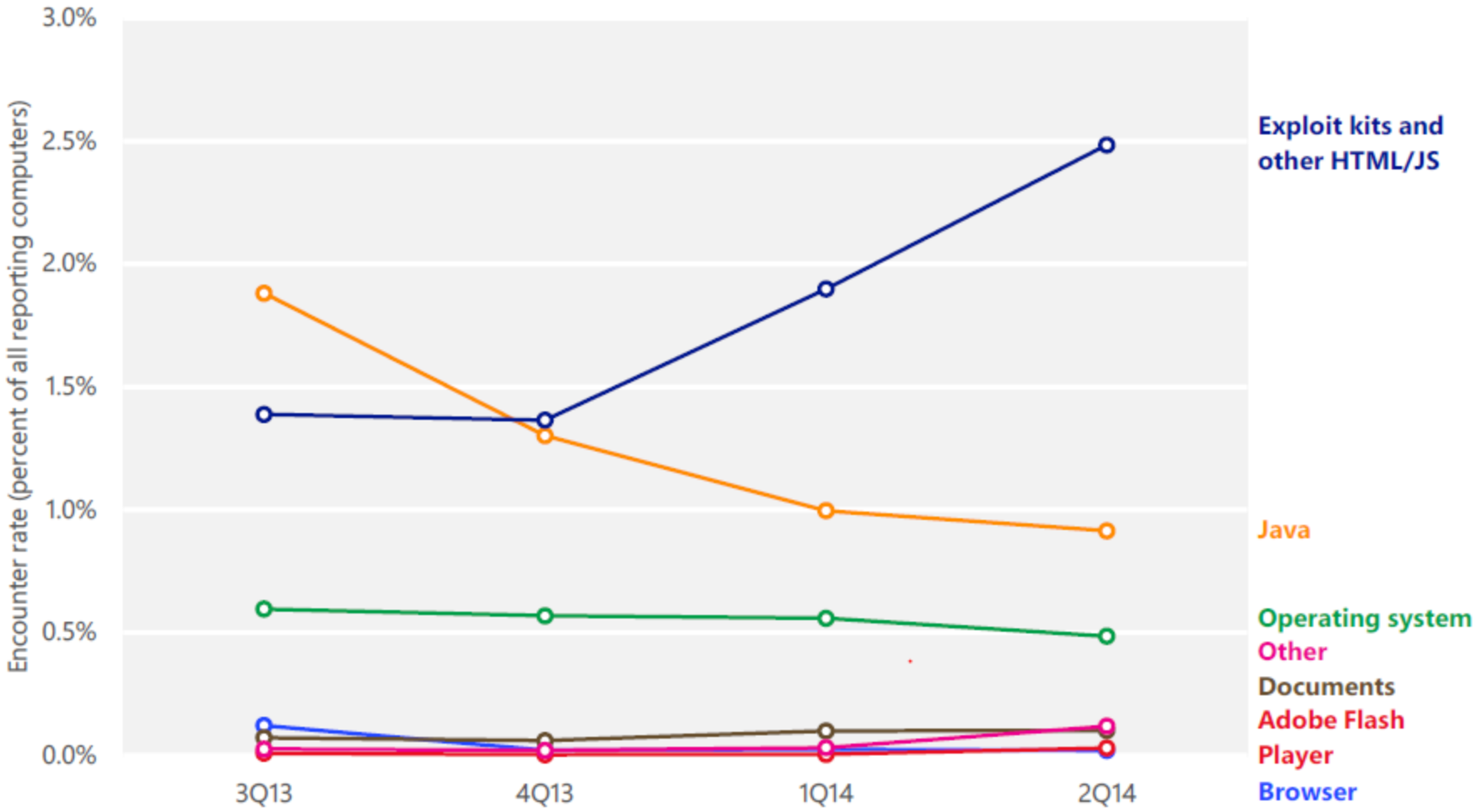
Figure 15. Industrywide vulnerability disclosures in 1H14, by severity



source: ***Microsoft Security Intelligence Report – Volume 17***

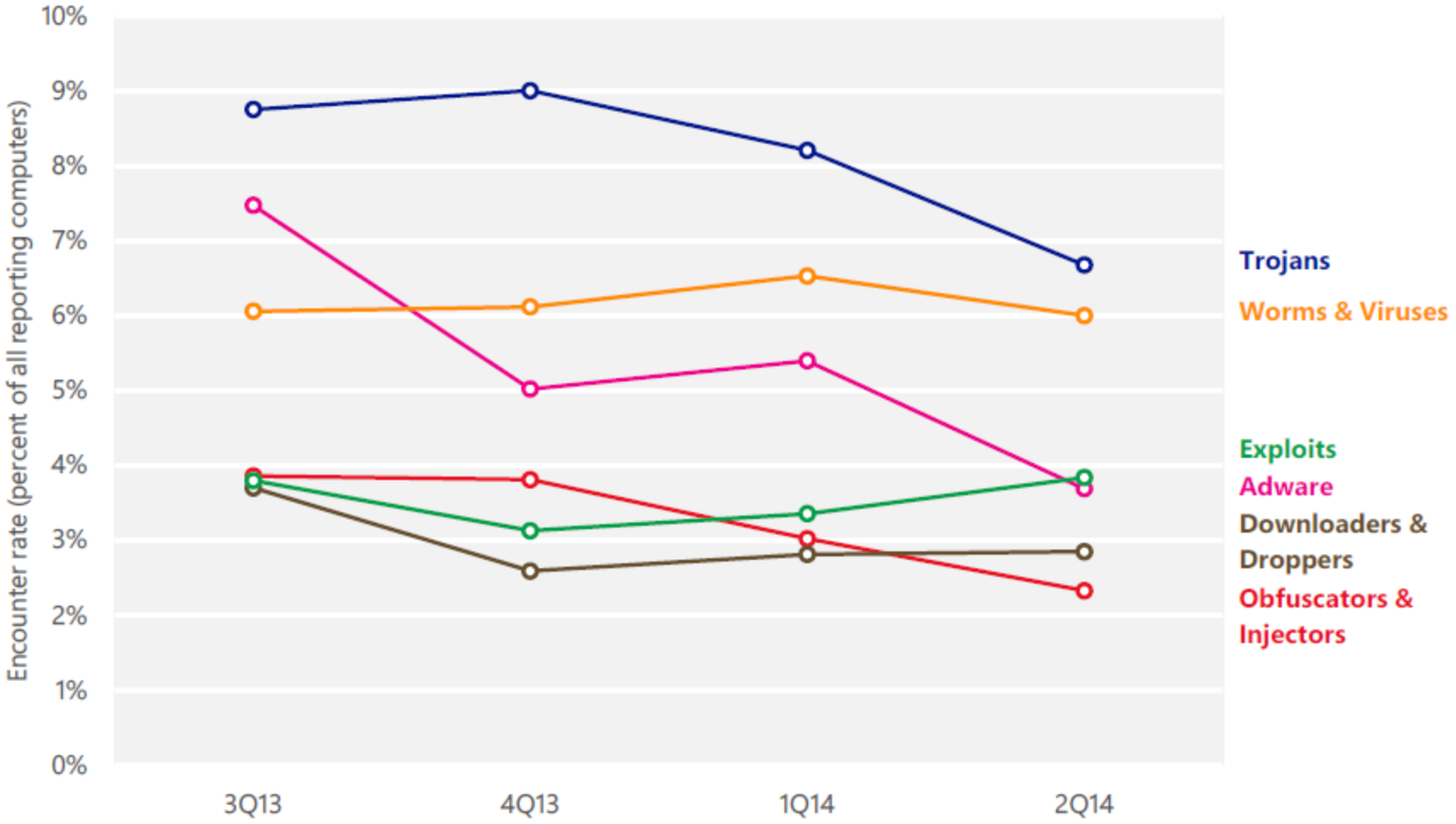
paloalto NETWORKS

Statistics: Type of exploits



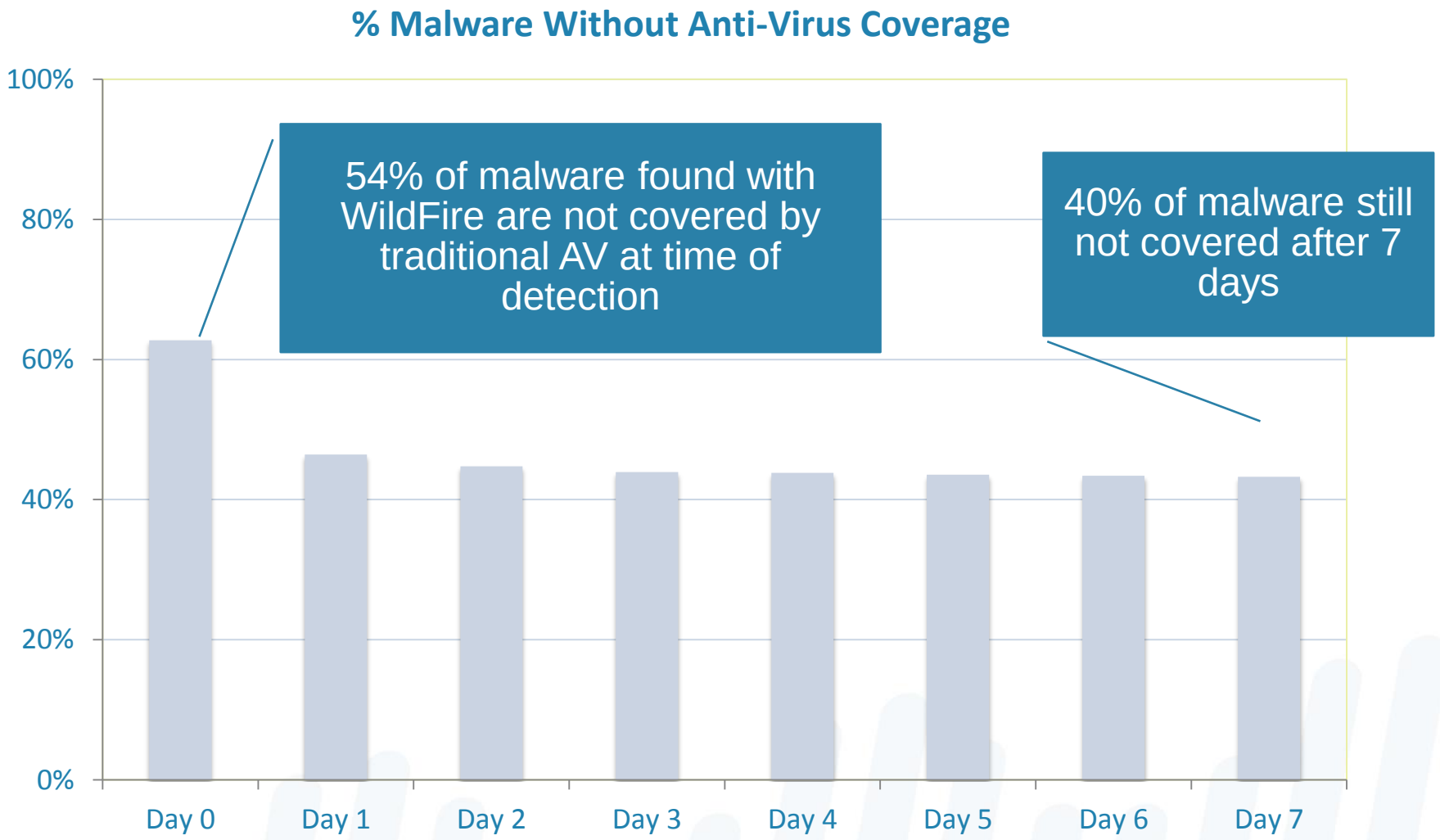
source: ***Microsoft Security Intelligence Report – Volume 17***

Statistics: Type of malware



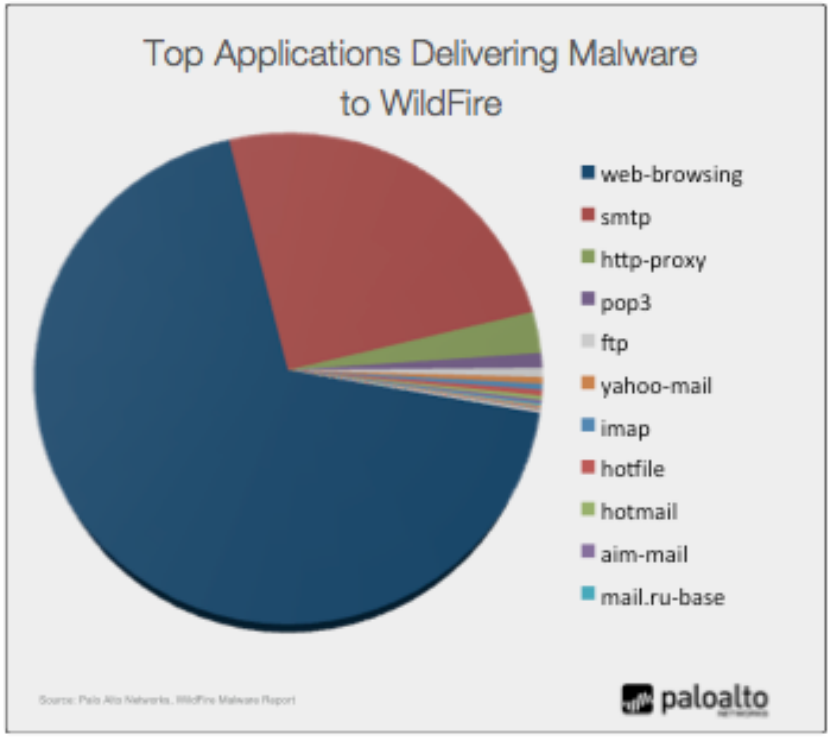
source: ***Microsoft Security Intelligence Report – Volume 17***

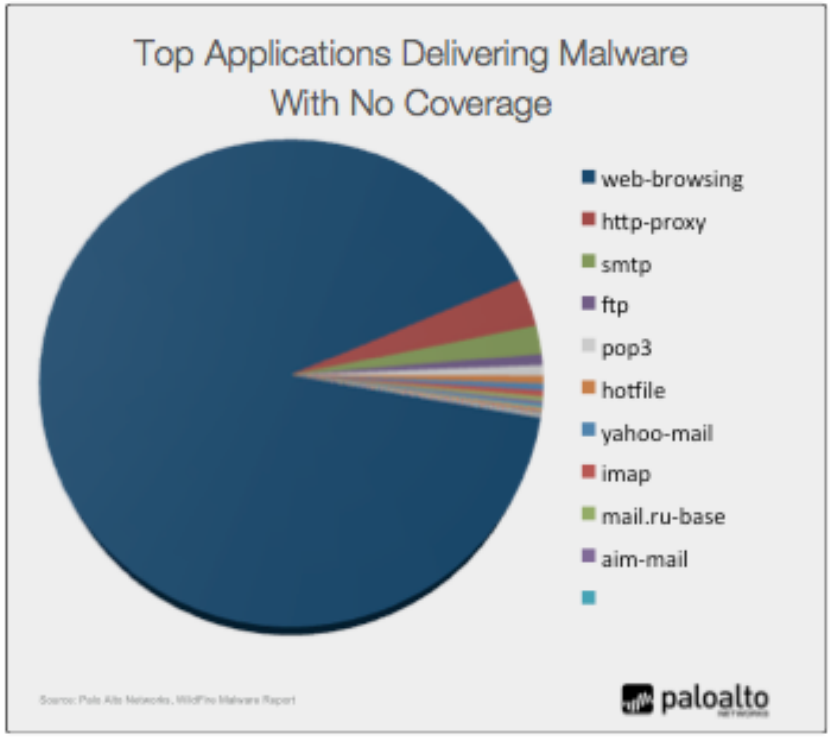
A New Breed of Malware



Attackvectors

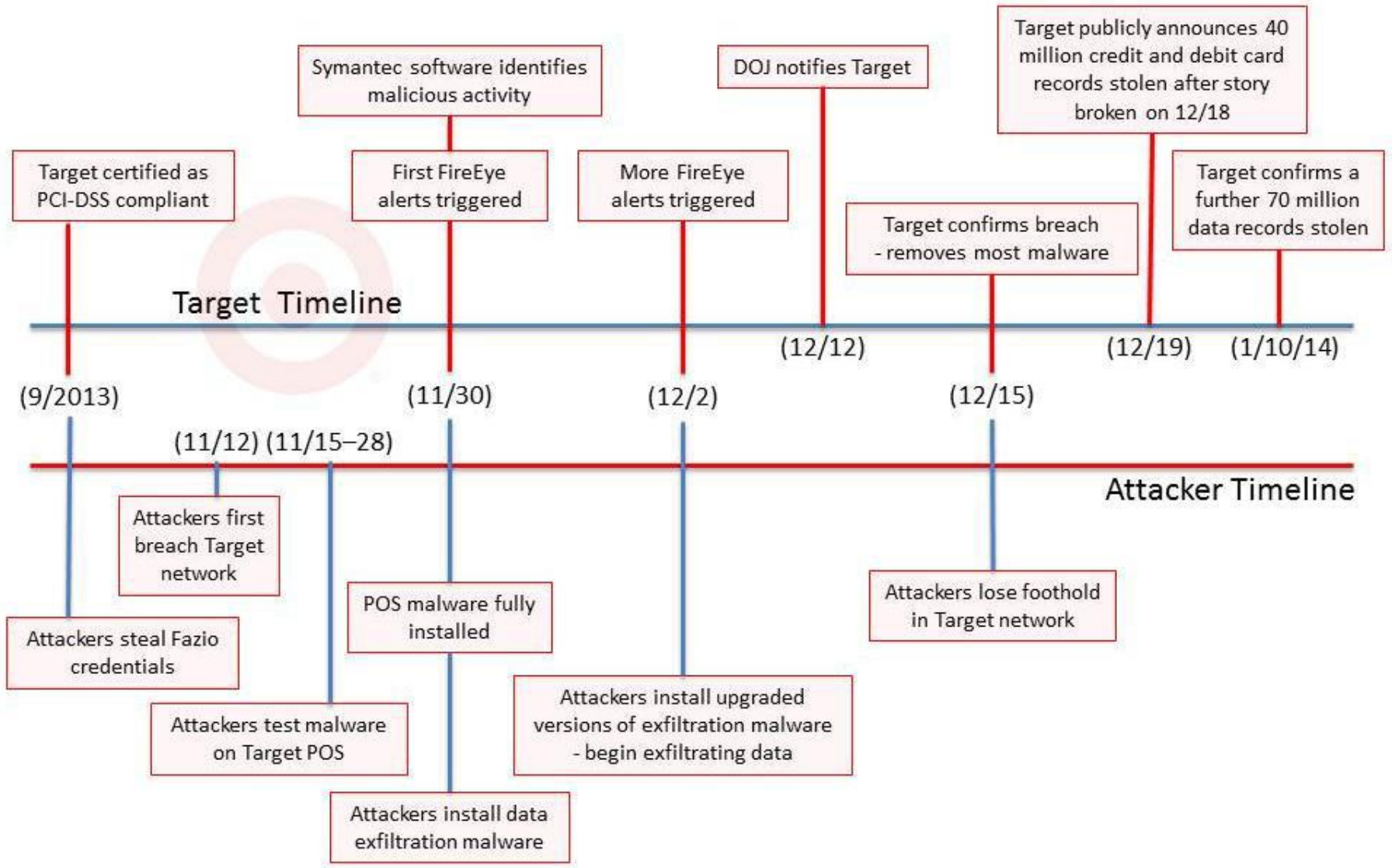
- The web is where the action is for unknown malware.





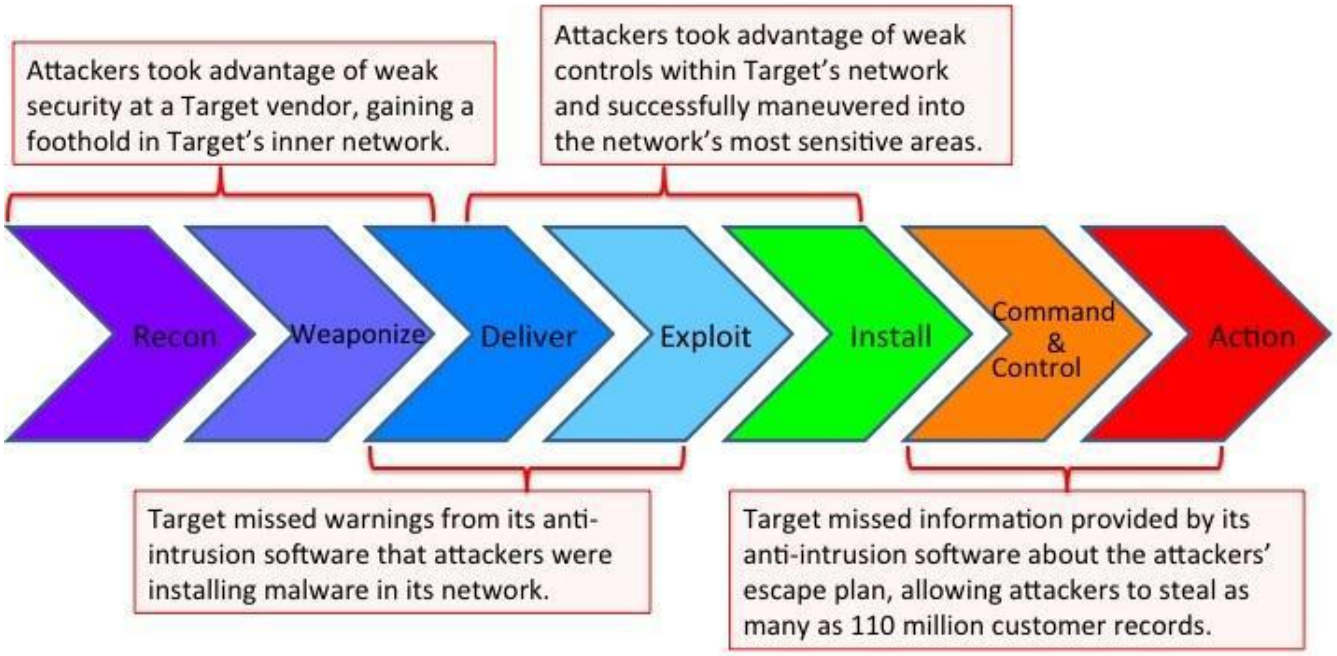
3% of malware delivered by email evaded all vendors
vs
More than 50% of malware delivered by the web

Target breach timeline



- Quote from Jayce Nichols, manager of cybercrime analysis team iSight

"The interesting thing is the way the attackers put everything together and the orchestration of the overall attack, not necessarily the sophistication of the individual components…"



The facts

The Facts Speak for Themselves

There is no such thing as perfect security. Attackers get smarter and change tactics all of the time.
Companies who have made responsible and sustained investments in IT continue to be compromised.

100%

of victims have up-to-date anti-virus software

63%

of breaches are reported by third parties

243

median number of days advanced attackers are on the network before being detected

100%

of breaches involved stolen credentials

from www.mandiant.com

Affected Software

CVE-2011-4162
CVE-2011-0611
CVE-2013-0640
CVE-2013-0641
…

CVE-2012-0422
CVE-2013-1493
CVE-2013-2423
…

CVE-2011-0609
CVE-2011-0611
CVE-2012-0779
CVE-2013-0630

CVE-2010-3333
CVE-2012-0158
CVE-2013-3847
…

CVE-2010-0249
CVE-2012-4792
CVE-2012-1347
…

paloalto NETWORKS

Exploit market

Netragard's founder Adriel Desautels says he's been in the exploit-selling game for a decade, and describes how the market has "exploded" in just the last year. He says there are now "more buyers, deeper pockets," that the time for a purchase has accelerated from months to weeks, and he's being approached by sellers with around 12 to 14 zero-day exploits every month compared to just four to six a few years ago.

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

And the latest (in case you missed it)

3.3.1 APT-Angriff auf Industrieanlagen in Deutschland

Sachverhalt

Gezielter Angriff auf ein Stahlwerk in Deutschland.

Methode

Mittels Spear-Phishing und ausgefeiltem Social Engineering erlangten Angreifer initialen Zugriff auf das Büronetz des Stahlwerks. Von dort aus arbeiteten sie sich sukzessive bis in die Produktionsnetze vor.

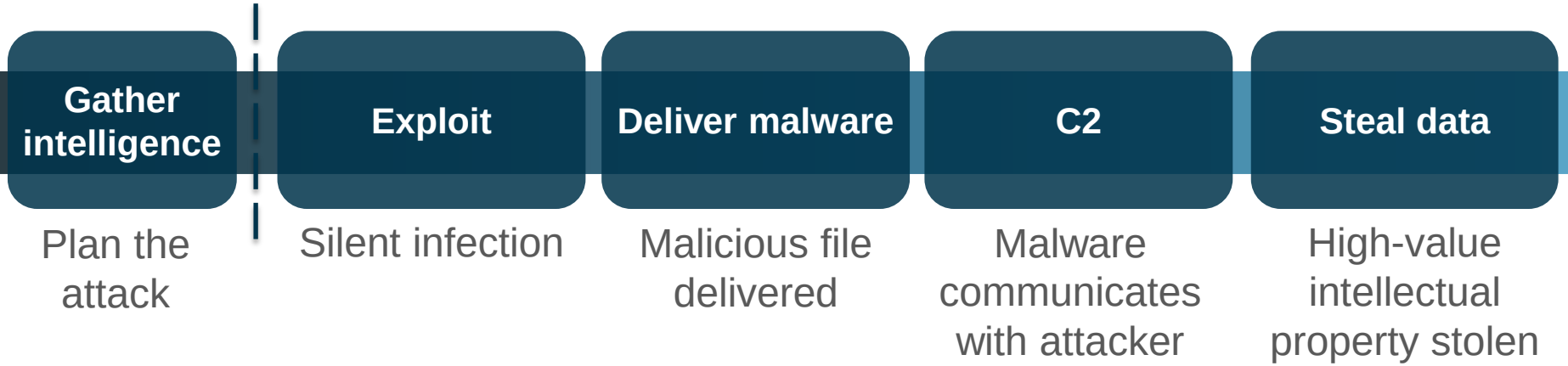
Schadenswirkung

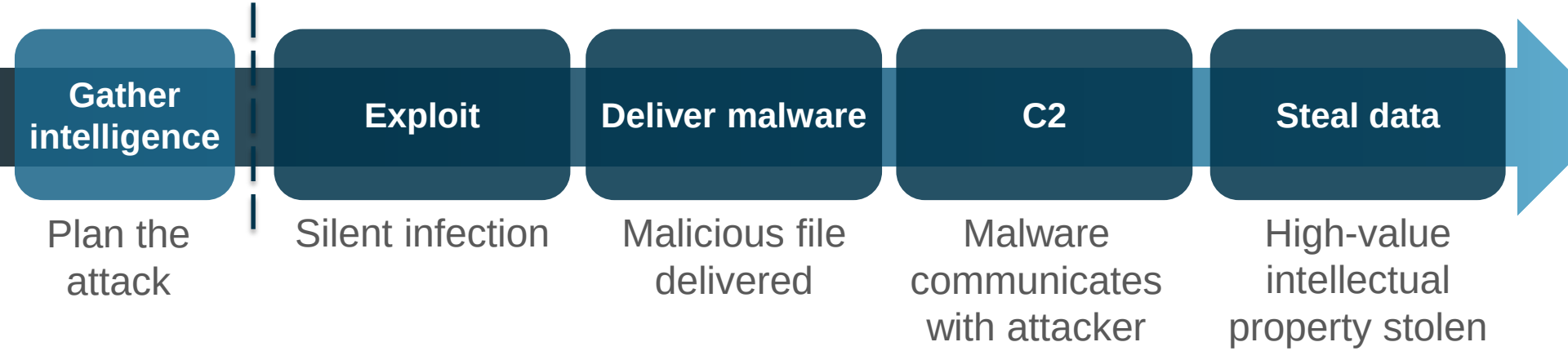
Es häuften sich Ausfälle einzelner Steuerungskomponenten oder ganzer Anlagen. Die Ausfälle führten dazu, dass ein Hochofen nicht geregelt heruntergefahren werden konnte und sich in einem undefinierten Zustand befand. Die Folge waren massive Beschädigungen der Anlage.

The good news

- To be successfull the attacker needs all steps
- To prevent, we only need to break one !

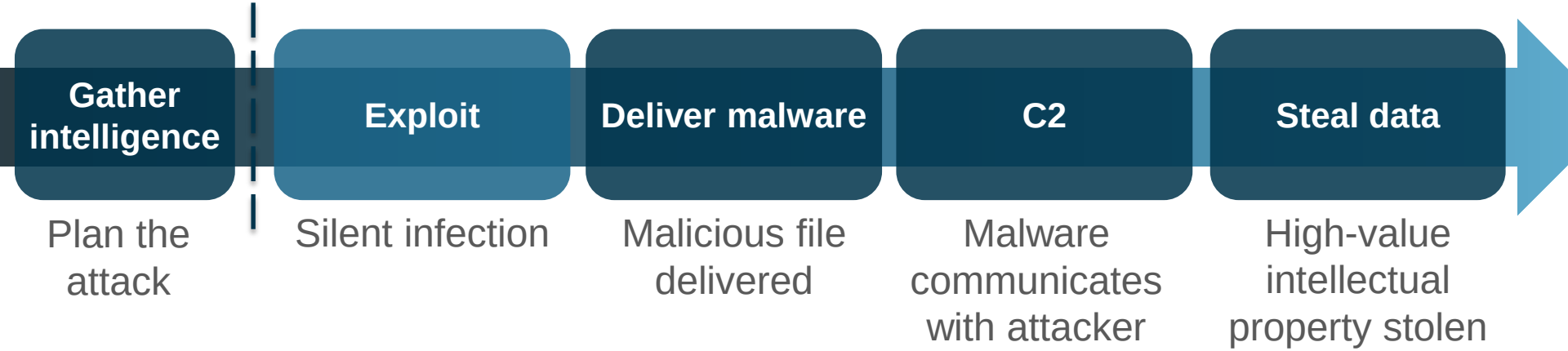
How to defeat such a Kill Chain





Stage 0 – Information gathering

- Lower the attack surface
  - User awareness, user awareness , user awareness , user awareness , user awareness ….



Stage 1 - Bait the user

- Lower the attack surface
  - Does your business really need to receive all file formats?
  - What is the business case for uninspectable content?
  - Why need all users full internet access?
  - User awareness, user awareness , user awareness ….

URLs obfuscation

- Use of strings that look good over IPs instead of names:

http://192.168.2.90/amazon/account_update/update-now

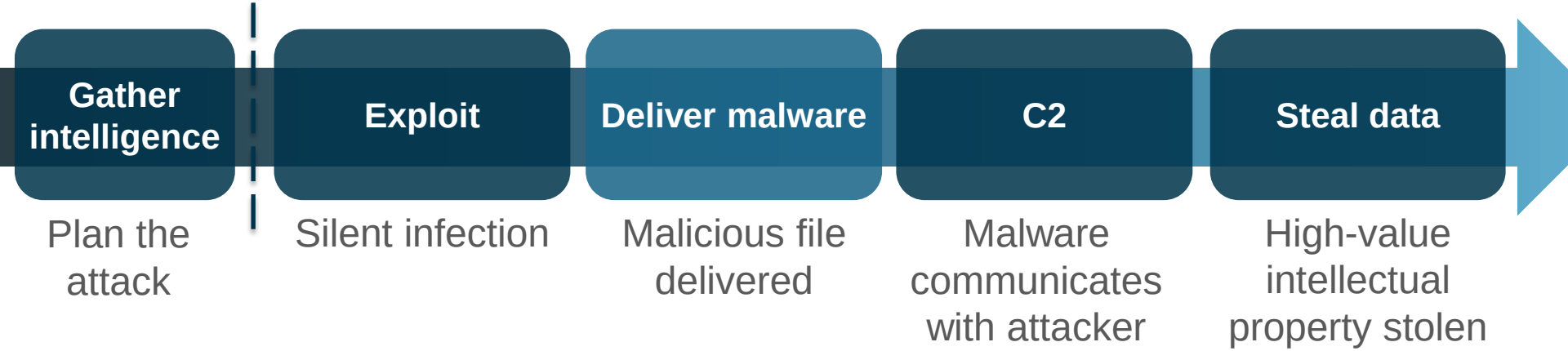
- Use of the @ symbol. Everything on the left side of @ is not used (detected by most modern browsers):

http://www.bbva.es/system/activate@192.168.2.90/vuln.php

- Use of lengthy strings so that they don't fit in the browser address bar.
- URL coding using hex, dword or octal:

http://%31%39%32%2e%31%36%38%2e%32%2e%39%30

(http://192.168.2.90)

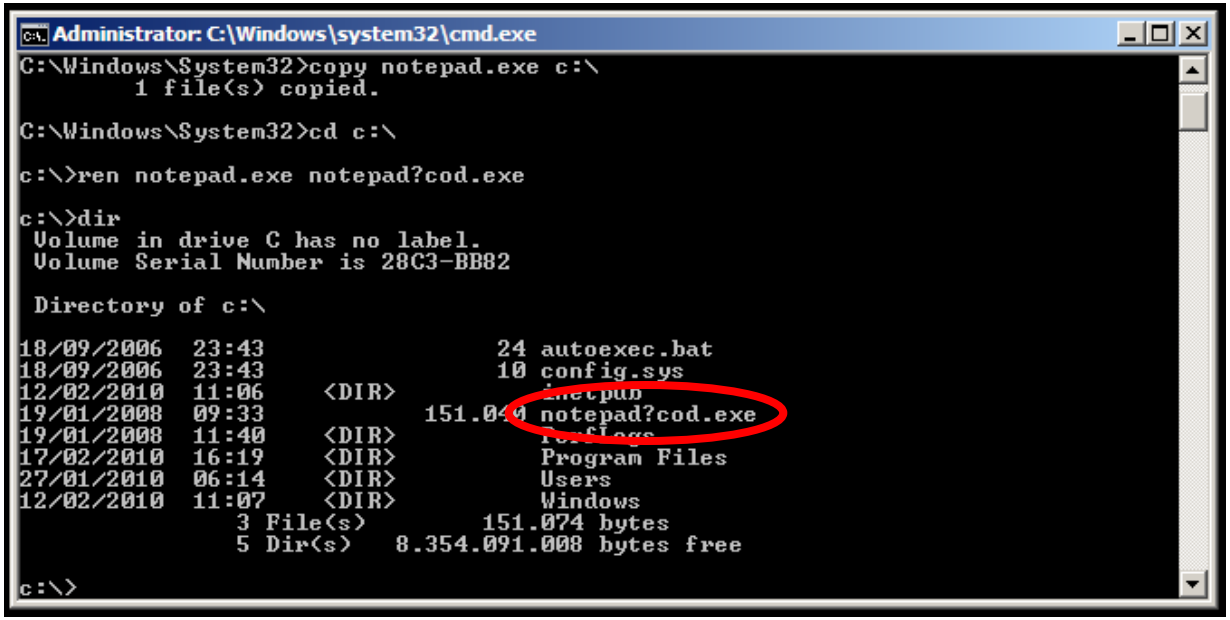


Stage 2 - exploit

- Block the know
  - Inspect everything, no exception!
  - Use up to date signatures

Hiding of real file extensions: Example

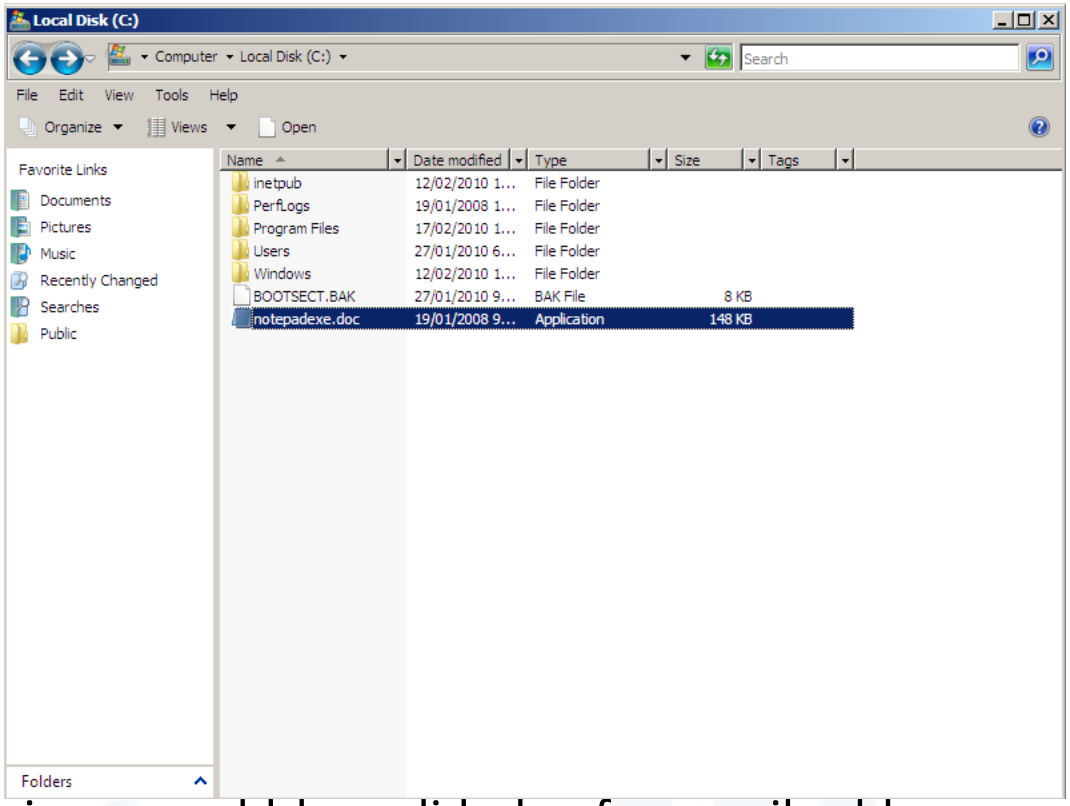
- After we rename the file chosing the right name. In our example we will rename “notepad.exe” as “notepad[U+202E]cod.exe”:



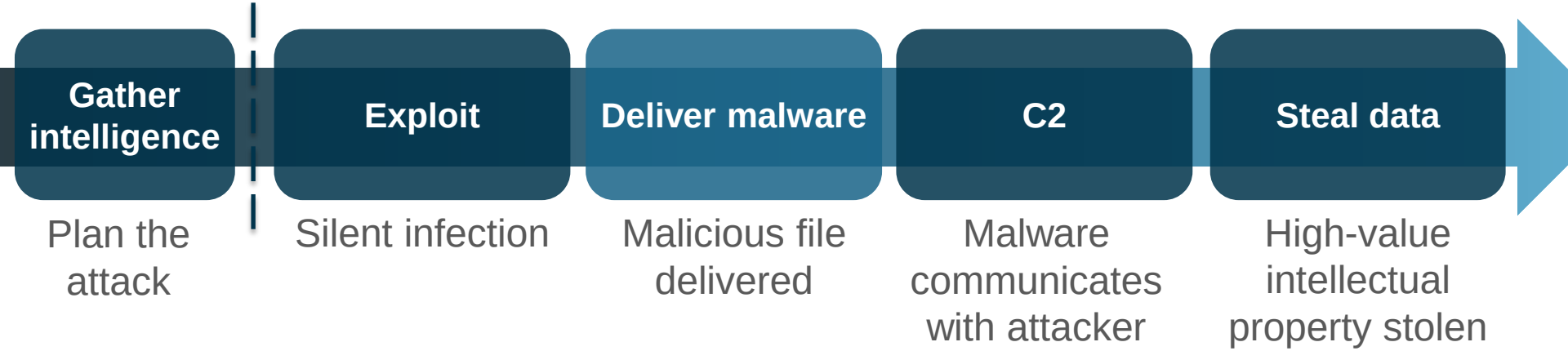
- Note that in the Windows CLI the file is properly displayed, including a ‘?’ character, representing the RTL one.

Hiding of real file extensions: Example

- On the other hand, and via the file explorer, the change works (modifying the icon would be trivial as well):

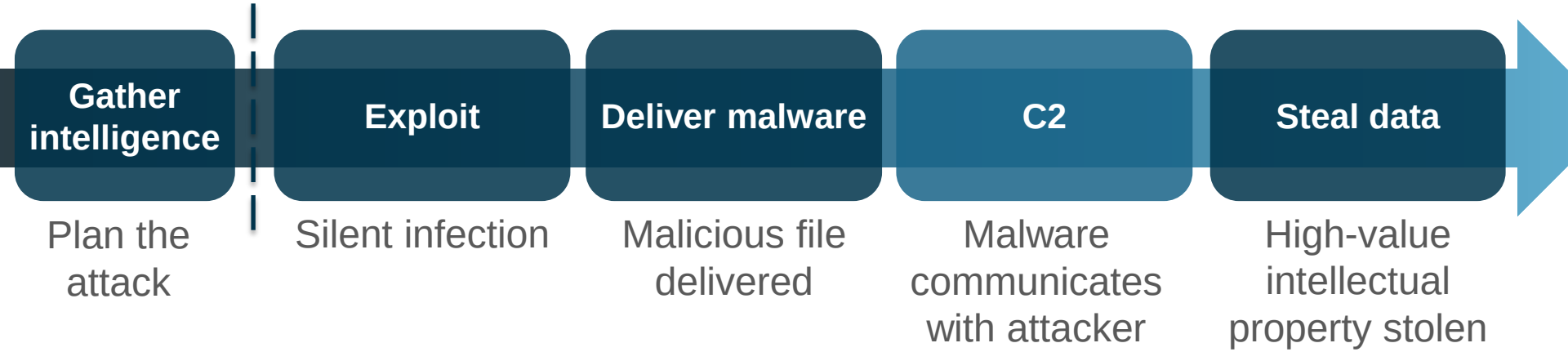


- These tecniques could be valid also for email addresses or URLs, depending on the client program that the end user is utilizing.



Stage 3 – download Backdoor

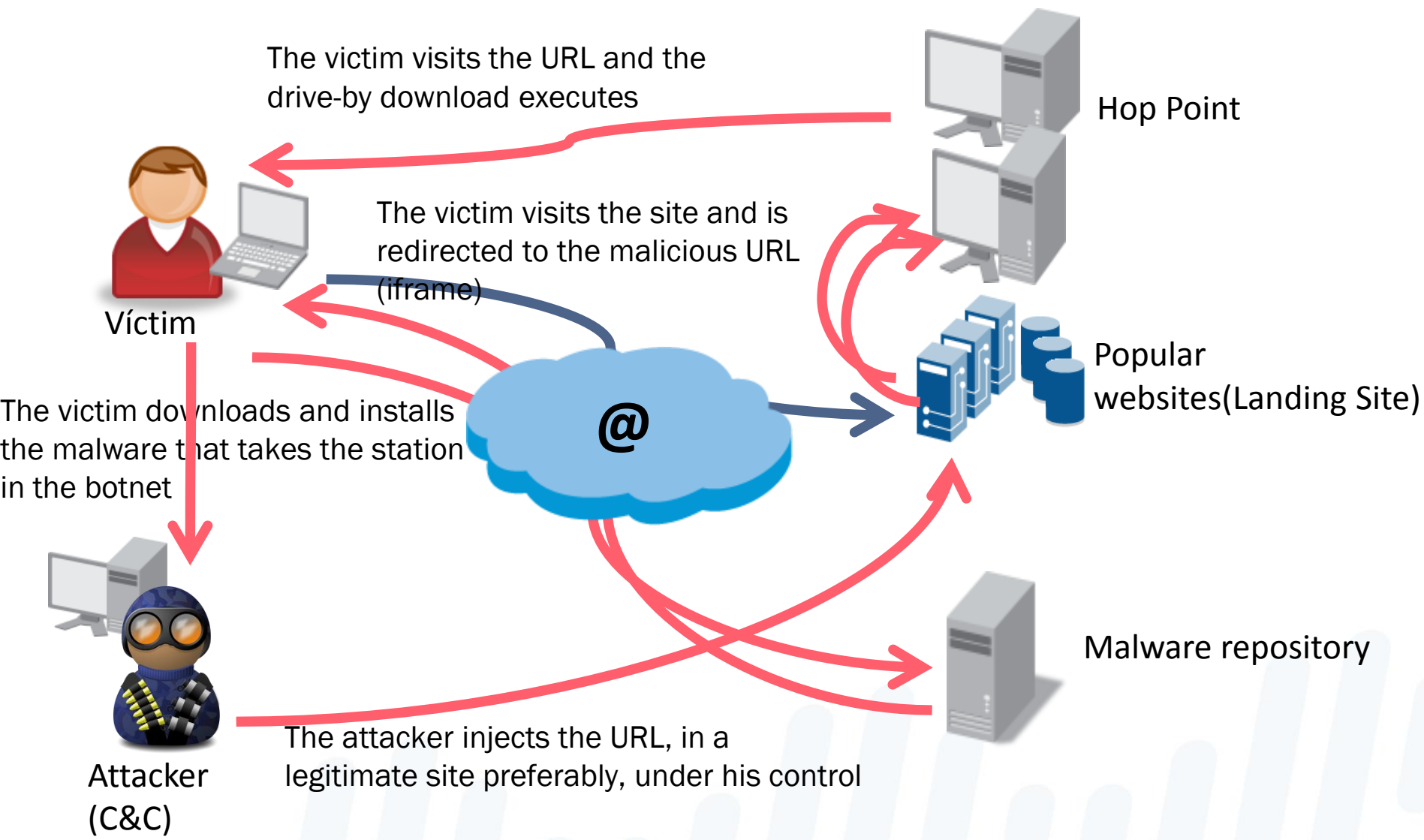
- Block the know
  - Inspect everything, no exception!
  - Use up to date signatures
- Prevent automatic downloads
- Analyze the suspicious
  - Try to turn the unknown into know



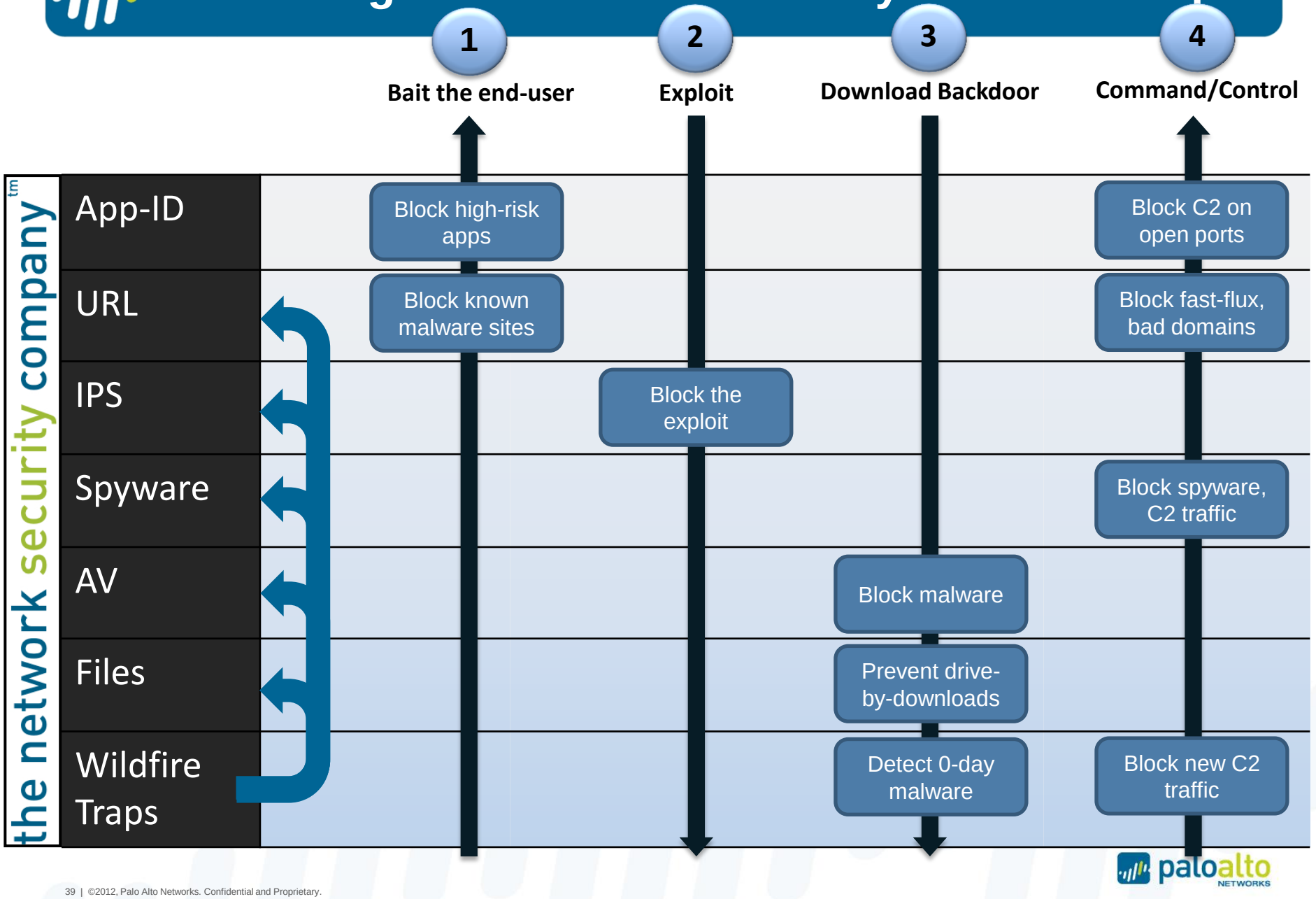
Stage 4 – Command/Control

- Only allow known and needed Application and block C2
- Leverage URL filtering to catch C2
- Why need all devices full internet access?
- Analyze the suspicious
  - Try to turn the unknown into know

Summary: Global flow



Breaking the Kill Chain at Every Possible Step

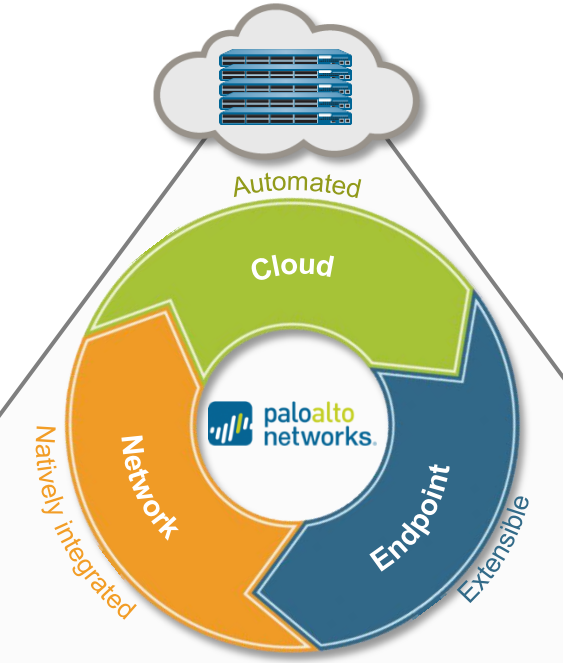


Copy the integrated approach

- Aggregate all information and defenses
- Leverage integrated systems

Integrated = More Than the Sum of It's Parts

Palo Alto Networks
Wildfire Analysis



Next-Generation Firewall

- **Erkennen** aller Anwendungen & User
- **Blocken** bekannter Bedrohungen
- **Verkleinerung** der Angriffsfläche

Threat Intelligence Cloud

- Analyse **unbekannter** Bedrohungen
- Automatisierte Erstellung von **Signaturen**
- **Aktualisierung** von Netzwerk und Endpunkt

Advanced Endpoint Protection

- **Untersucht** Prozesse & Files
- **Verhindert** bekannte und unbekannte Bedrohungen

Palo Alto Networks
Next-Generation Firewall

Palo Alto Networks
Advanced Endpoint Protection

paloalto NETWORKS

And most important – Forensic Readyness

The following ten steps describe the key activities in implementing a forensic readiness programme.

1. Define the business scenarios that require digital evidence.
2. Identify available sources and different types of potential evidence.
3. Determine the evidence collection requirement.
4. Establish a capability for securely gathering legally admissible evidence to meet the requirement.
5. Establish a policy for secure storage and handling of potential evidence.
6. Ensure monitoring is targeted to detect and deter major incidents.
7. Specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched.
8. Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence.
9. Document an evidence-based case describing the incident and its impact.
10. Ensure legal review to facilitate action in response to the incident.

Conclusions

- Evolution of your Network Security
  - Limited IOC action ability with Islands of Technology
  - Market acceptance of our Core Platform Values
- It's a new Threat Landscape
  - New motivations… financial, intelligence
  - Hacker's tools have evolved… evasive
- Need for an integrated approach
  - Traditional solutions no longer suffice
  - Focus on breaking the Kill Chain, not just on the point-attack

Questions ?

Thank you

- Enjoy the networking

