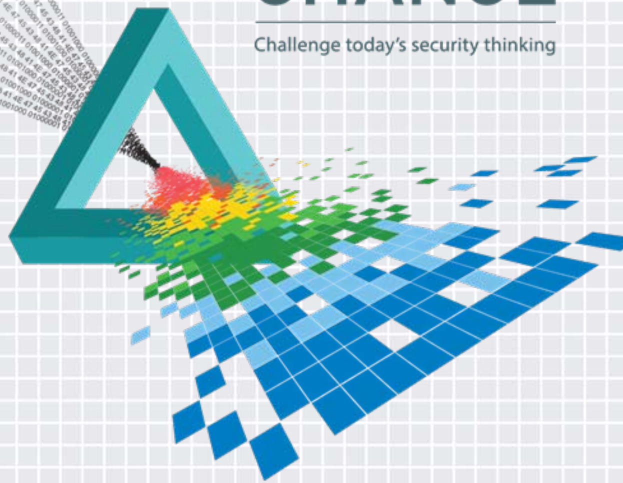
RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking



SESSION ID: SPO2-R02

Advanced Attacks: How One Exploited Endpoint Leads to Total Datacenter Breach

Nati Davidi

VP, Product Management
Palo Alto Networks
@NatiDavidi

Sebastian Goodwin

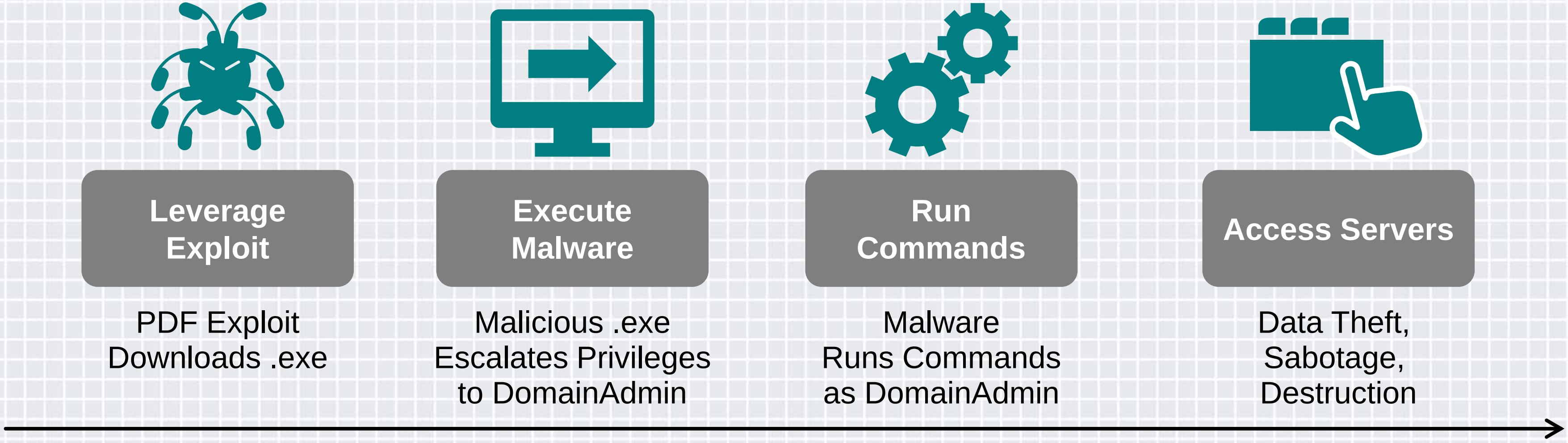
Director, Endpoint Initiatives
Palo Alto Networks
@SebGoodSF

#RSAC

It All Begins with One Endpoint

- The adversary’s path of least resistance begins with an endpoint.
- AV and network-based controls are not able to prevent an advanced targeted exploit attack on an endpoint.
- Once the endpoint is compromised, the adversary has a clear path to privilege escalation and access to the datacenter.
- Advanced Endpoint Protection is needed to prevent such attacks at the earliest possible stage.

Overview of the Attack



Leverage Exploit

PDF Exploit Downloads .exe

Execute Malware

Malicious .exe Escalates Privileges to DomainAdmin

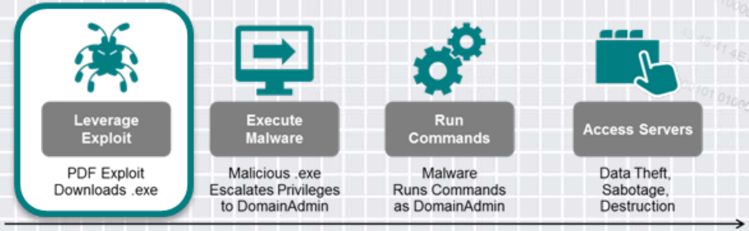
Run Commands

Malware Runs Commands as DomainAdmin

Access Servers

Data Theft, Sabotage, Destruction

Prevention of the Attack at the Earliest Stage is Critical



Leverage Exploit
PDF Exploit Downloads .exe

Execute Malware
Malicious .exe Escalates Privileges to DomainAdmin

Run Commands
Malware Runs Commands as DomainAdmin

Access Servers
Data Theft, Sabotage, Destruction

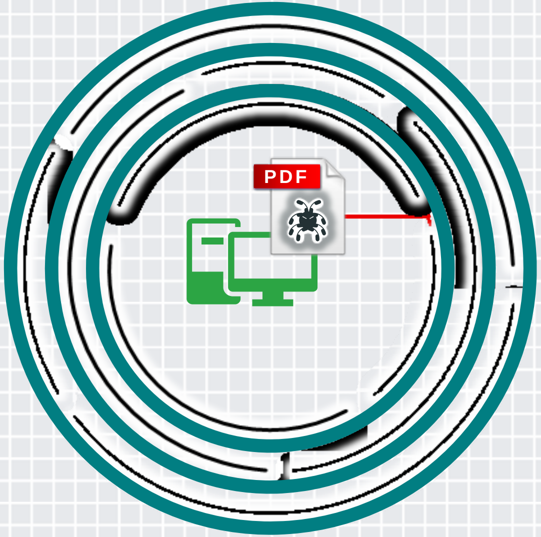
#RSAC

Stop the attack before it begins: Exploit Prevention

Advanced Endpoint Protection

The Right Way to Deal with Advanced Cyber Threats

- Prevent Exploits – Including zero-day exploits
- Prevent Malicious Executables– Including advanced and unknown malware
- Collect Attempted-Attack Forensics – For further analysis
- Scalable, Lightweight, Full Coverage – Apply protection to any application with minimal user impact
- Integrate with Network and Cloud Security – For data exchange and cross-organization protection



Block the Core Techniques – Not the Individual Attacks

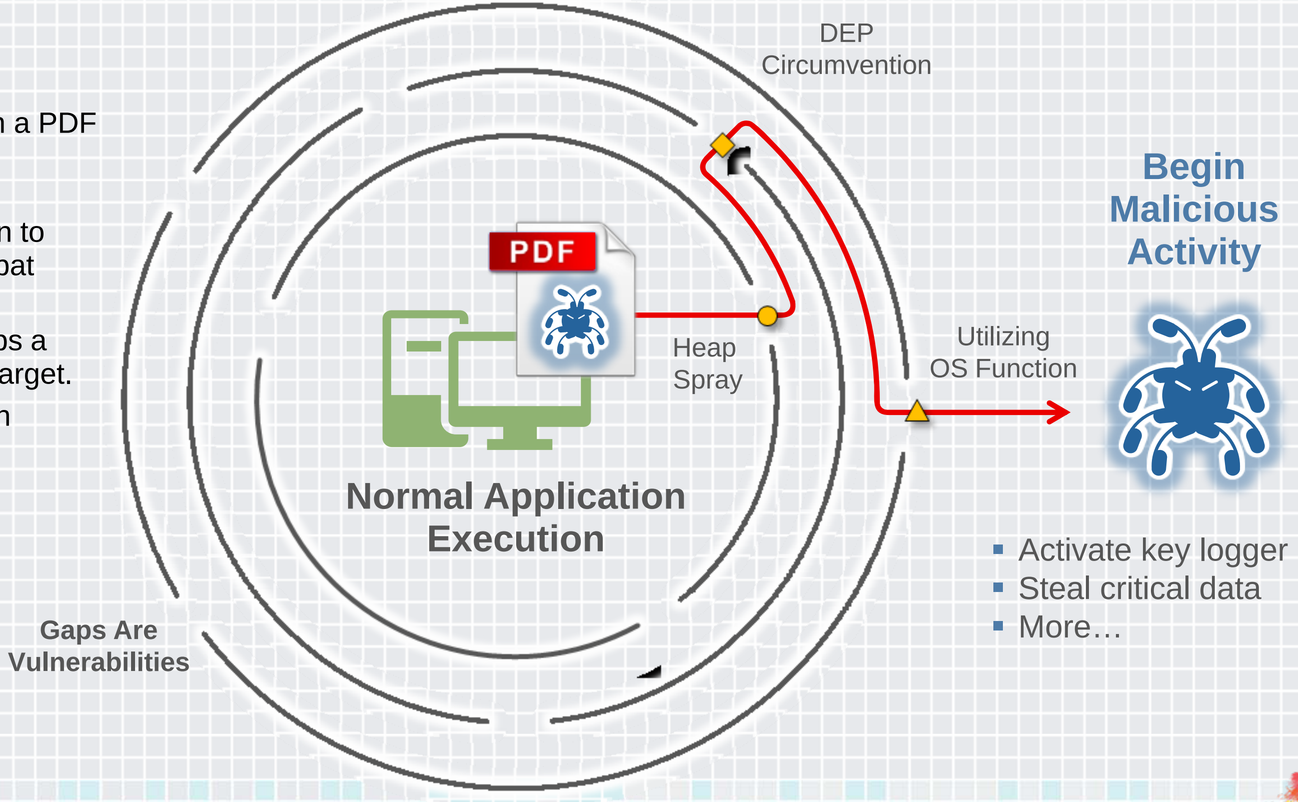
Number of New Variants Each Year

Individual Attacks	Core Techniques
1,000s **Software Vulnerability Exploits** Thousands of new vulnerabilities and exploits	**2-4** **Exploitation Techniques** Only two to four new exploit techniques
1,000,000s **Malware** Millions of new malware variations	**~10s** **Malware Techniques** Tens of new malware sub-techniques

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…

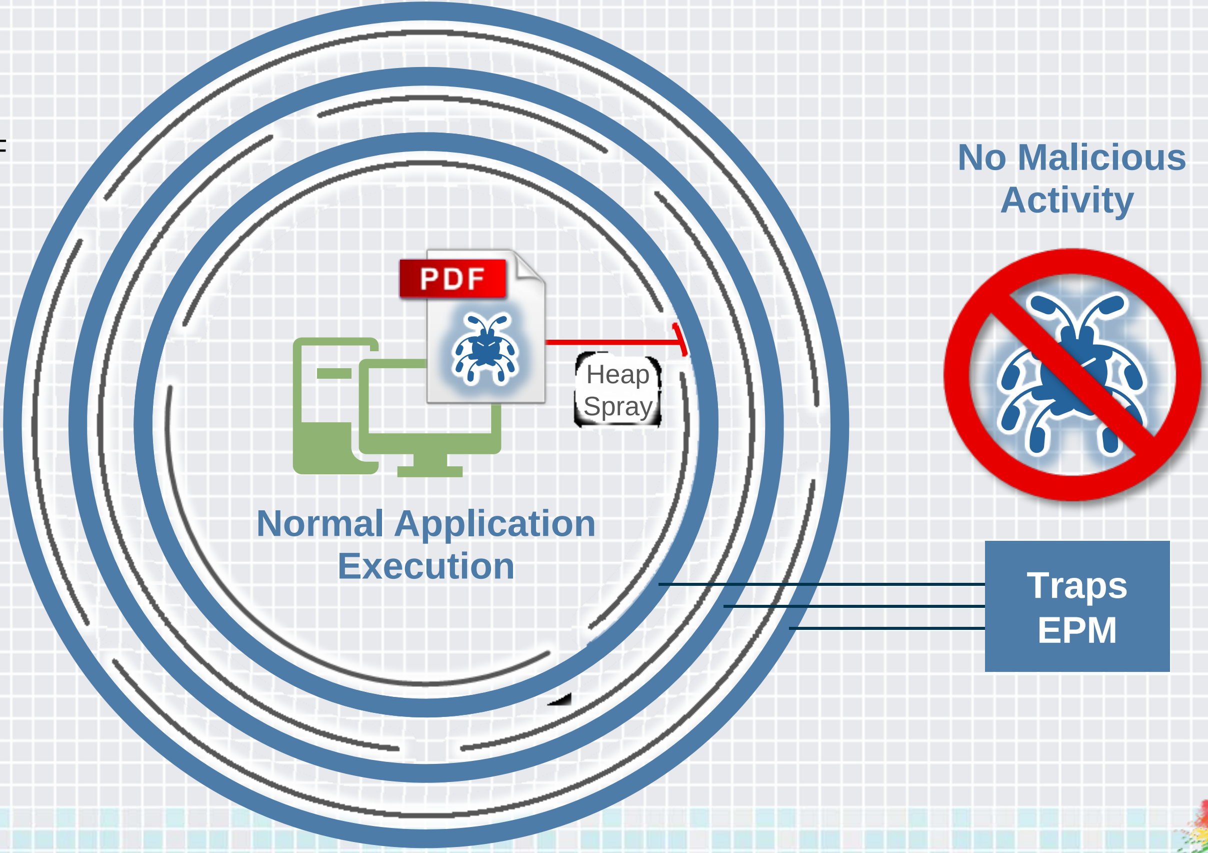
Exploit Techniques

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.

Traps Exploit Prevention Modules (EPM)

1. Exploit attempt blocked. Traps requires no prior knowledge of the vulnerability.



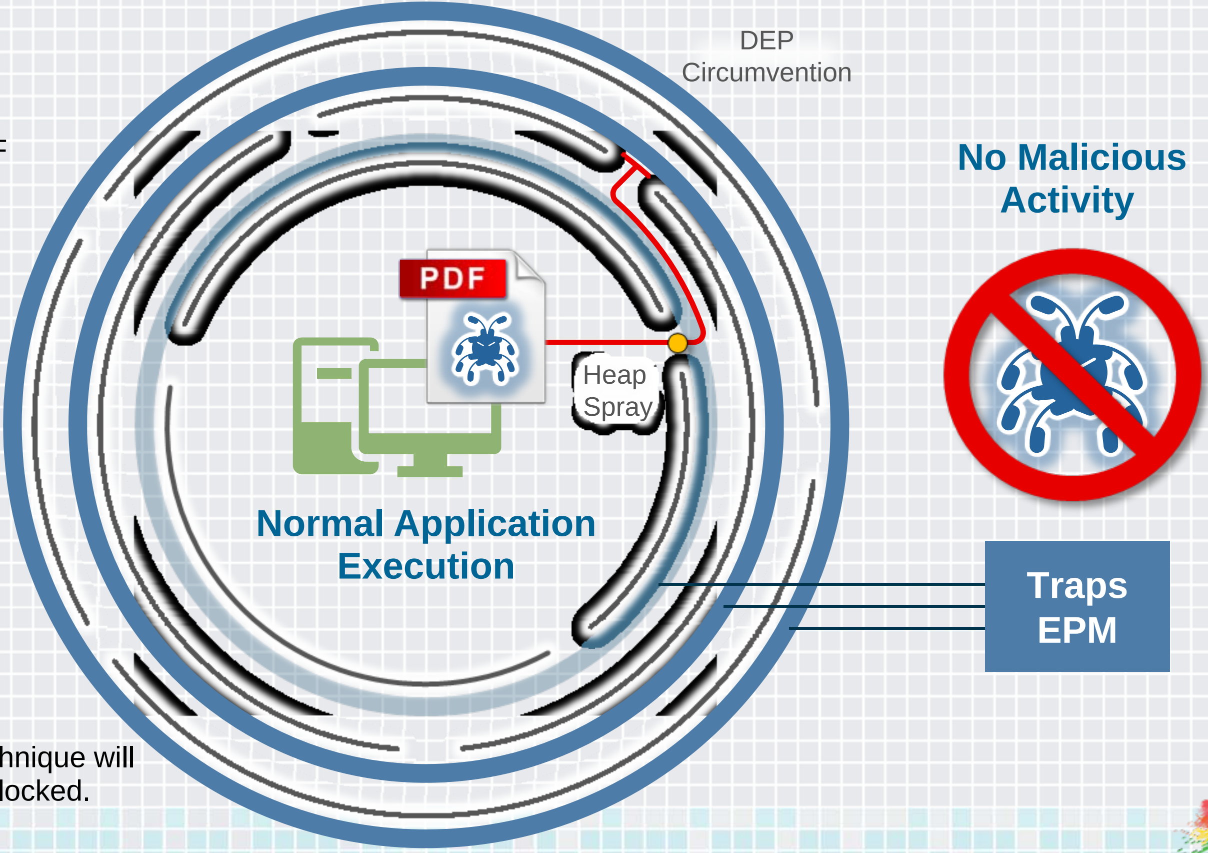
Exploit Techniques

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.

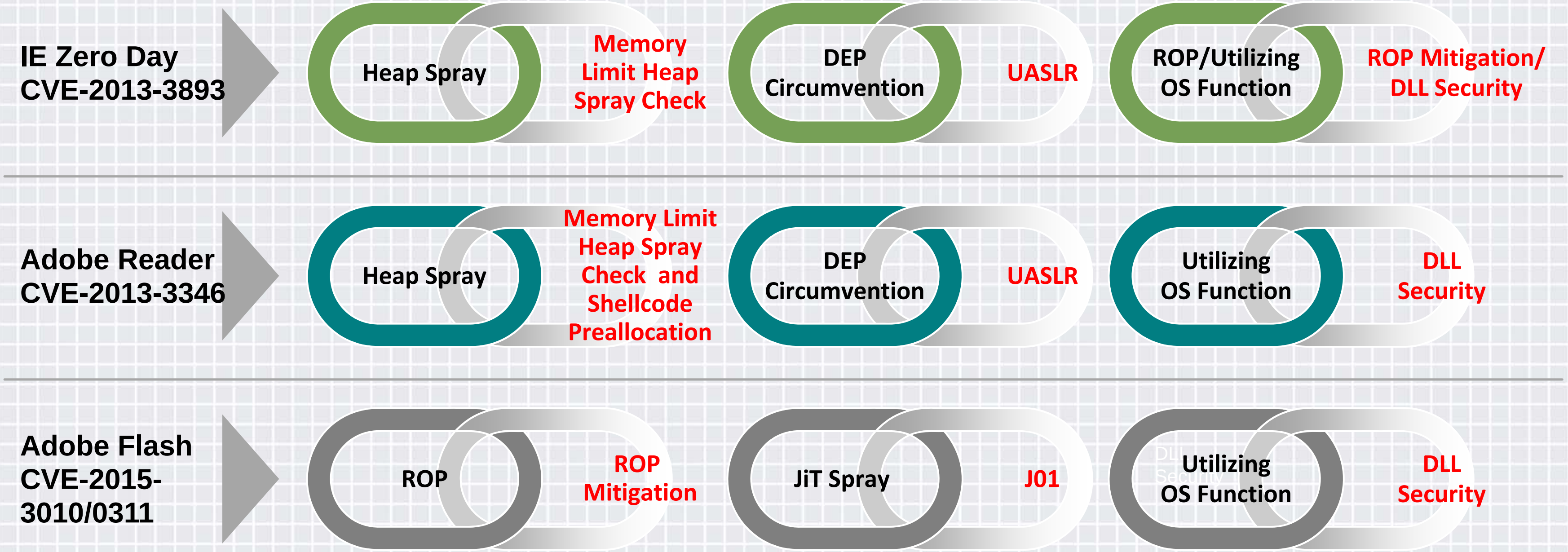
Traps Exploit Prevention Modules (EPM)

1. Exploit attempt blocked. Traps requires no prior knowledge of the vulnerability.
2. If you turn off EPM #1, the first technique will succeed but the next one will be blocked.



Exploit Prevention Case Study

Unknown Exploits Utilize Known Techniques



IE Zero Day
CVE-2013-3893

Heap Spray

Memory Limit Heap Spray Check

DEP Circumvention

UASLR

ROP/Utilizing OS Function

ROP Mitigation/ DLL Security

Adobe Reader
CVE-2013-3346

Heap Spray

Memory Limit Heap Spray Check and Shellcode Preallocation

DEP Circumvention

UASLR

Utilizing OS Function

DLL Security

Adobe Flash
CVE-2015-3010/0311

ROP

ROP Mitigation

JiT Spray

J01

DLL Security

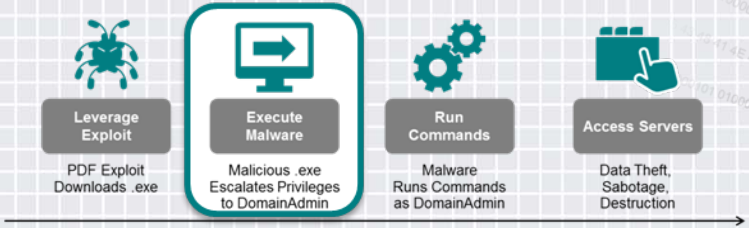
Utilizing OS Function

DLL Security

Prevention of One Technique in the Chain will Block the Entire Attack

RSAConference2015

San Francisco | April 20-24 | Moscone Center


Leverage Exploit
PDF Exploit Downloads .exe
Execute Malware
Malicious .exe Escalates Privileges to DomainAdmin
Run Commands
Malware Runs Commands as DomainAdmin
Access Servers
Data Theft, Sabotage, Destruction

Prevent Unknown Malware (Malicious Executables)

#RSAC

Preventing Malicious Executables on All Fronts

Advanced Execution Control

Reduce surface area of attack. Control execution scenarios based on file location, device, child processes, unsigned executables.

Local hash control allows for granular system hardening.

WildFire Inspection and Analysis

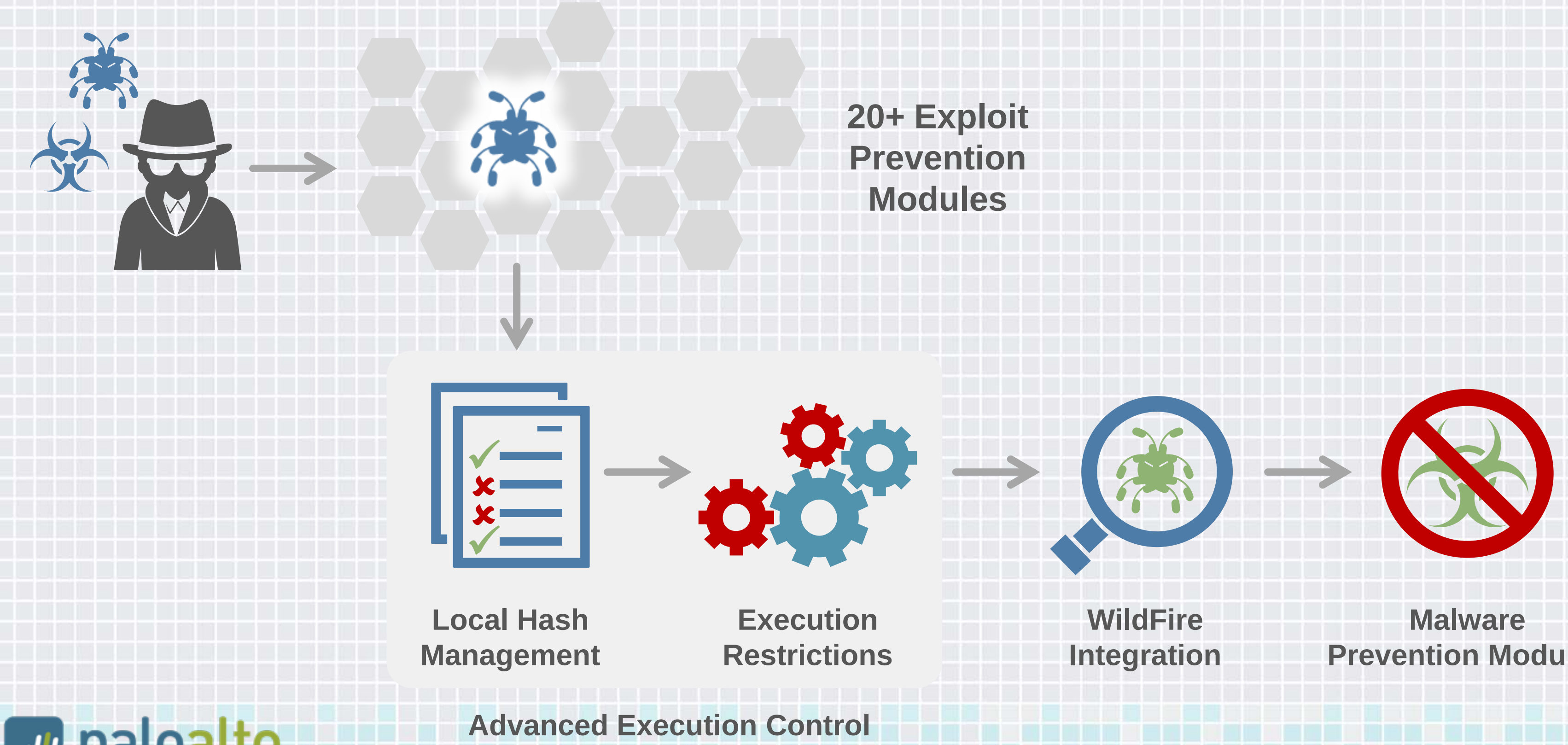
Dynamic analysis with cloud-based threat intelligence.

61% of malicious files identified by WildFire are not detected by the top 6 enterprise AV products.

Malware Techniques Mitigation

Prevent unknown malware with technique-based mitigation. (Example: Thread Injection)

The Most Comprehensive Approach to Endpoint Protection



20+ Exploit Prevention Modules

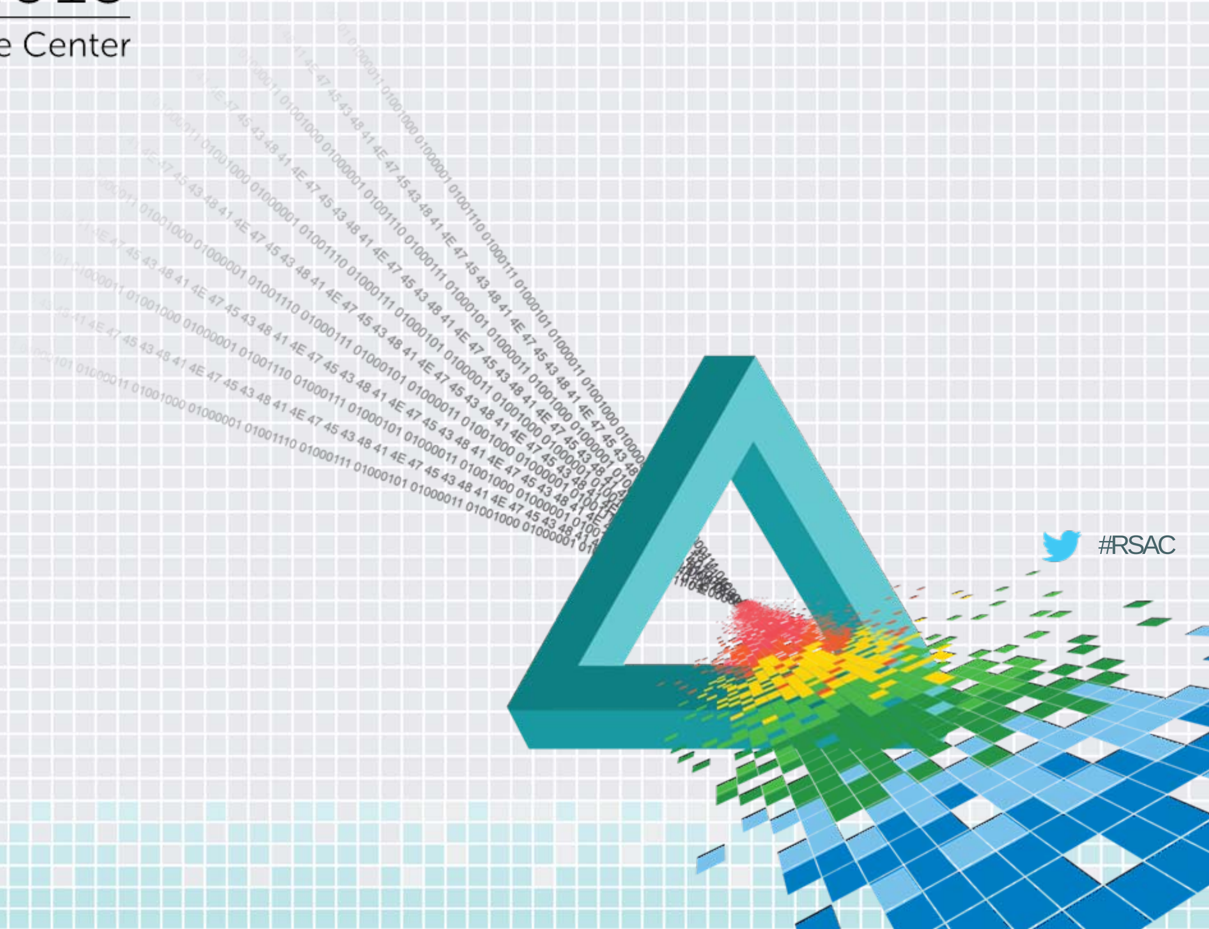
Local Hash Management

Execution Restrictions

WildFire Integration

Malware Prevention Modules

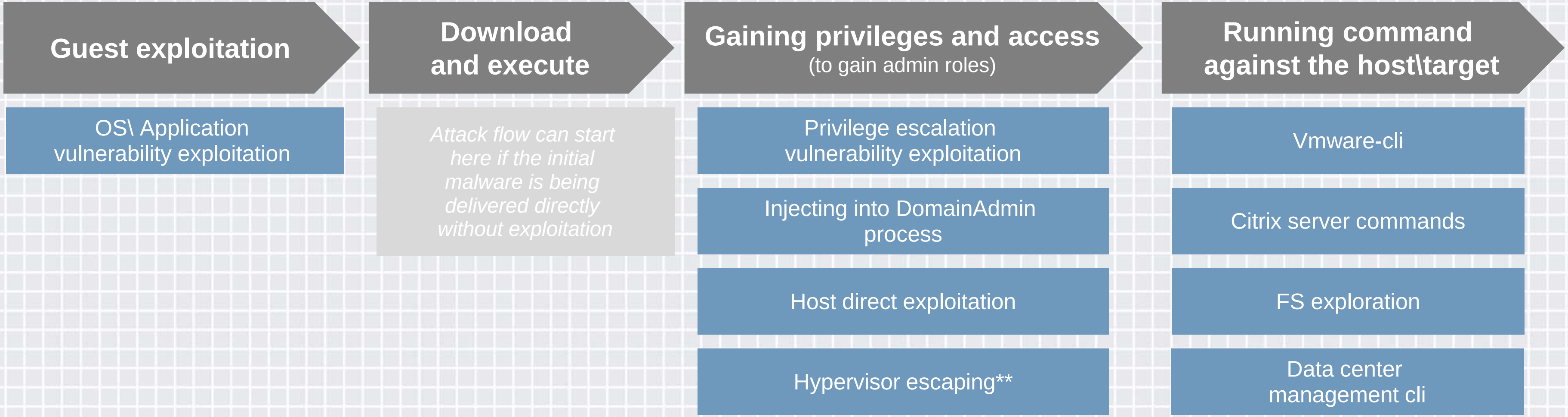
Advanced Execution Control



Demonstration

Compromising the host through guest exploitation

Demo



Guest exploitation

OS\ Application vulnerability exploitation

Download and execute

Attack flow can start here if the initial malware is being delivered directly without exploitation

Gaining privileges and access
(to gain admin roles)

Privilege escalation vulnerability exploitation

Injecting into DomainAdmin process

Host direct exploitation

Hypervisor escaping**

Running command against the host\target

Vmware-cli

Citrix server commands

FS exploration

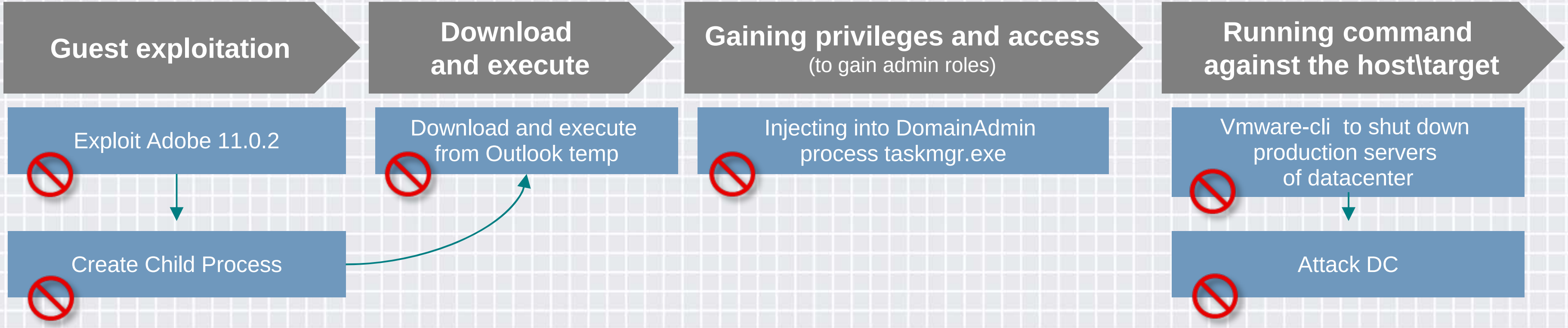
Data center management cli

** See Palo Alto Networks session “virtually impossible”

http://2013.zeronights.org/includes/docs/Gal_Diskin_-_Virtually_Impossible_-_ZeroNights_release_version.pdf

Compromising the host through guest exploitation

Demo



Guest exploitation

Exploit Adobe 11.0.2 🚫

Create Child Process 🚫

Download and execute

Download and execute from Outlook temp 🚫

Gaining privileges and access
(to gain admin roles)

Injecting into DomainAdmin process taskmgr.exe 🚫

Running command against the host\target

Vmware-cli to shut down production servers of datacenter 🚫

Attack DC 🚫

Apply What You’ve Learned

- If you’re still paying for endpoint AV, question that strategy. Your free options are roughly equivalent to your paid options in terms of ineffectiveness.
- Investigate endpoint security solutions that **prevent** known and unknown exploits and malware
- Protect **all** of your endpoints with advanced endpoint protection. Breach of one workstation can lead to total datacenter breach.