Cryptolocker
Anatomia di un attacco
Strategie di difesa e ripristino

Alessandro Ghezzi

Sr System Engineer, Symantec Italia

Agenda

- La minaccia Ransomware, un affare fiorente per i criminali
- Modalità operative e tecniche d’attacco utilizzate
- Fermare i Ransomware
- Q&A

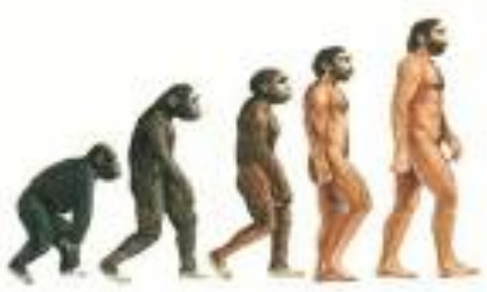
La minaccia Ransomware, un affare fiorente per i criminali

Il primo Ransomware “noto” della storia:

- 1989 ‘**PC Cyborg**’, autore il biologo Joseph Popp
- Cifratura a chiave simmetrica
- Sostituzione del file AUTOEXEC.BAT
- Cifratura di tutti i file presenti sull’unità C
- riscatto 189$ (importi incassati devoluti poi alla lotta contro l’AIDS)

L’evoluzione della “specie”:

- 2006 - Gpcode, TROJ.RANSOM.A, Archiveus, Krotten, Cryzip, e MayArchive
  - Cifratura a chiave asimmetrica, RSA a 660 bit, RSA a 1024 bit.
- **2013 - CryptoLocker**!!!,
  - Il primo ad usare i Bitcoin per il pagamento
- 2014 – 2015, CTB-Locker, Teslacrypt,Cryptowall,
  - RSA 2048, Crittografia Ellittica, Rete TOR per la comunicazione verso i C&C
- 2016 - Petya
  - Cifratura dell’MFT
- 2016 - **CTB-Locker WEB , Ke-Ranger**
  - Target WordPress sites, Mac OSx
- 2016 **Flocker**
  - Android, Smart-TV



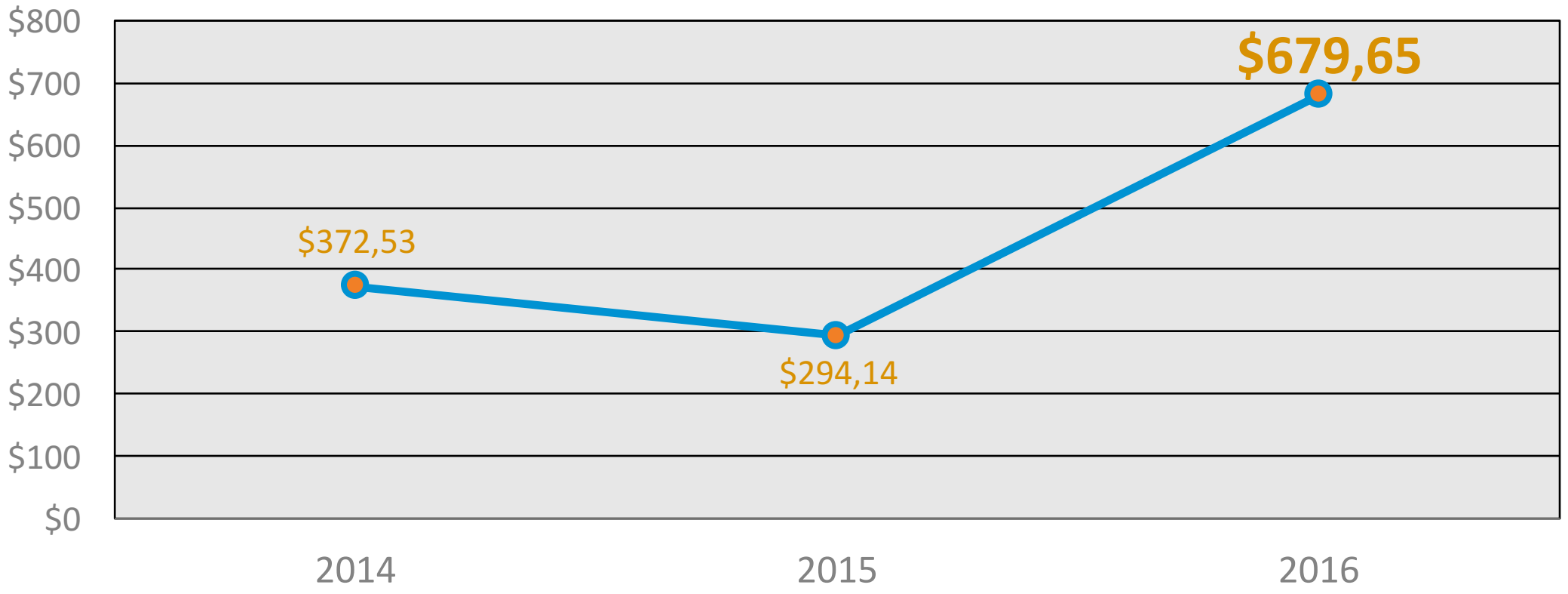
Ransomware Famiglie

100 nuove famiglie identificate nel 2015
contro 77 nel 2014

Ransomware fattori di crescita

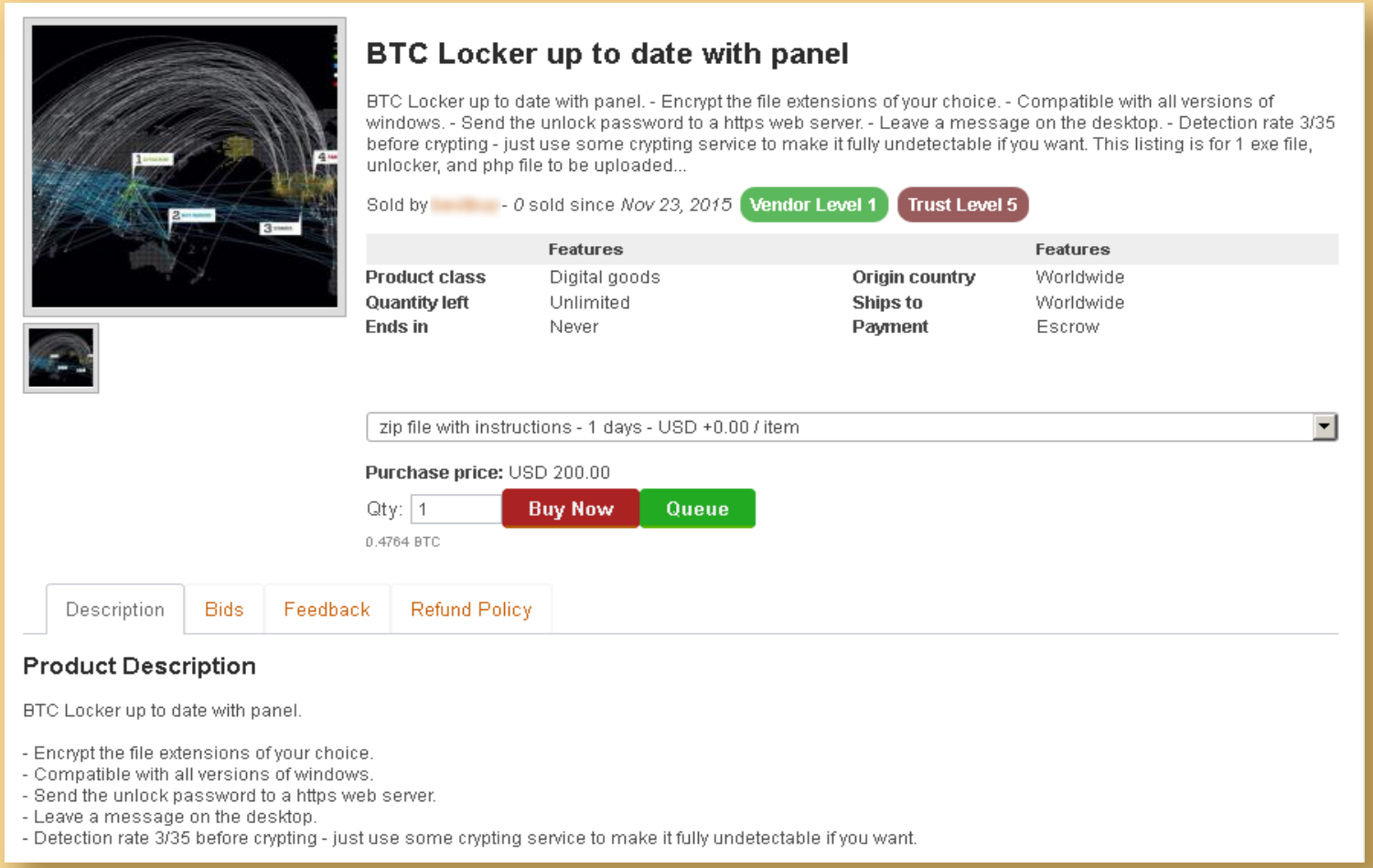
- Facilità d’accesso alle librerie di cifratura
- Vettori di infezione efficaci
- L'adozione di tecniche d’attacco avanzate
- Ransomware as a service

Richieste di riscatto



Le richieste medie di riscatto sono raddoppiate

Ransomware venduti nell'underground per $200



BTC Locker up to date with panel

BTC Locker up to date with panel. - Encrypt the file extensions of your choice. - Compatible with all versions of windows. - Send the unlock password to a https web server. - Leave a message on the desktop. - Detection rate 3/35 before crypting - just use some crypting service to make it fully undetectable if you want. This listing is for 1 exe file, unlocker, and php file to be uploaded...

Sold by [redacted] - *0* sold since *Nov 23, 2015* Vendor Level 1 Trust Level 5

	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

zip file with instructions - 1 days - USD +0.00 / item

Purchase price: USD 200.00

Qty: 1 Buy Now Queue

0.4764 BTC

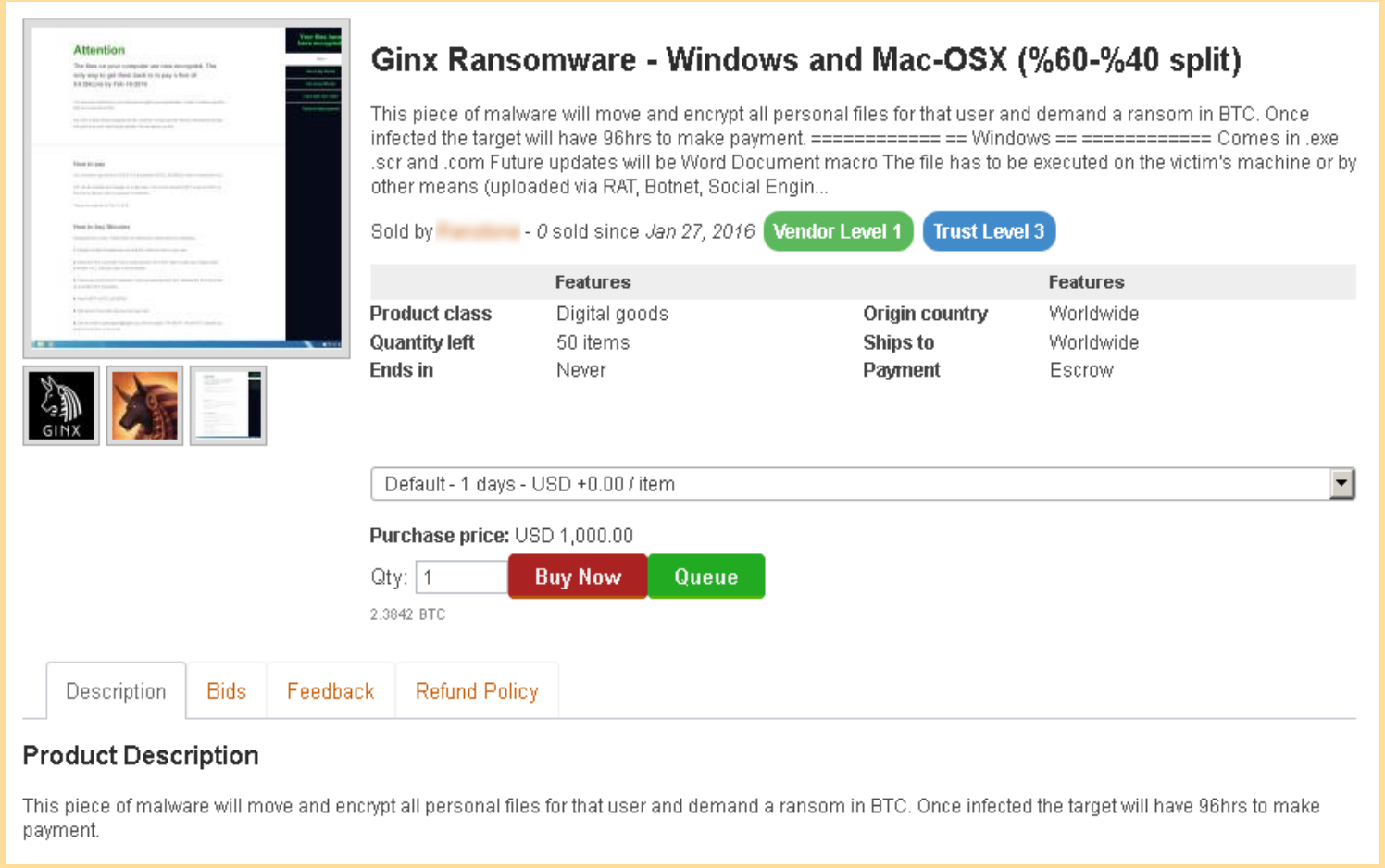
Description | Bids | Feedback | Refund Policy

Product Description

BTC Locker up to date with panel.

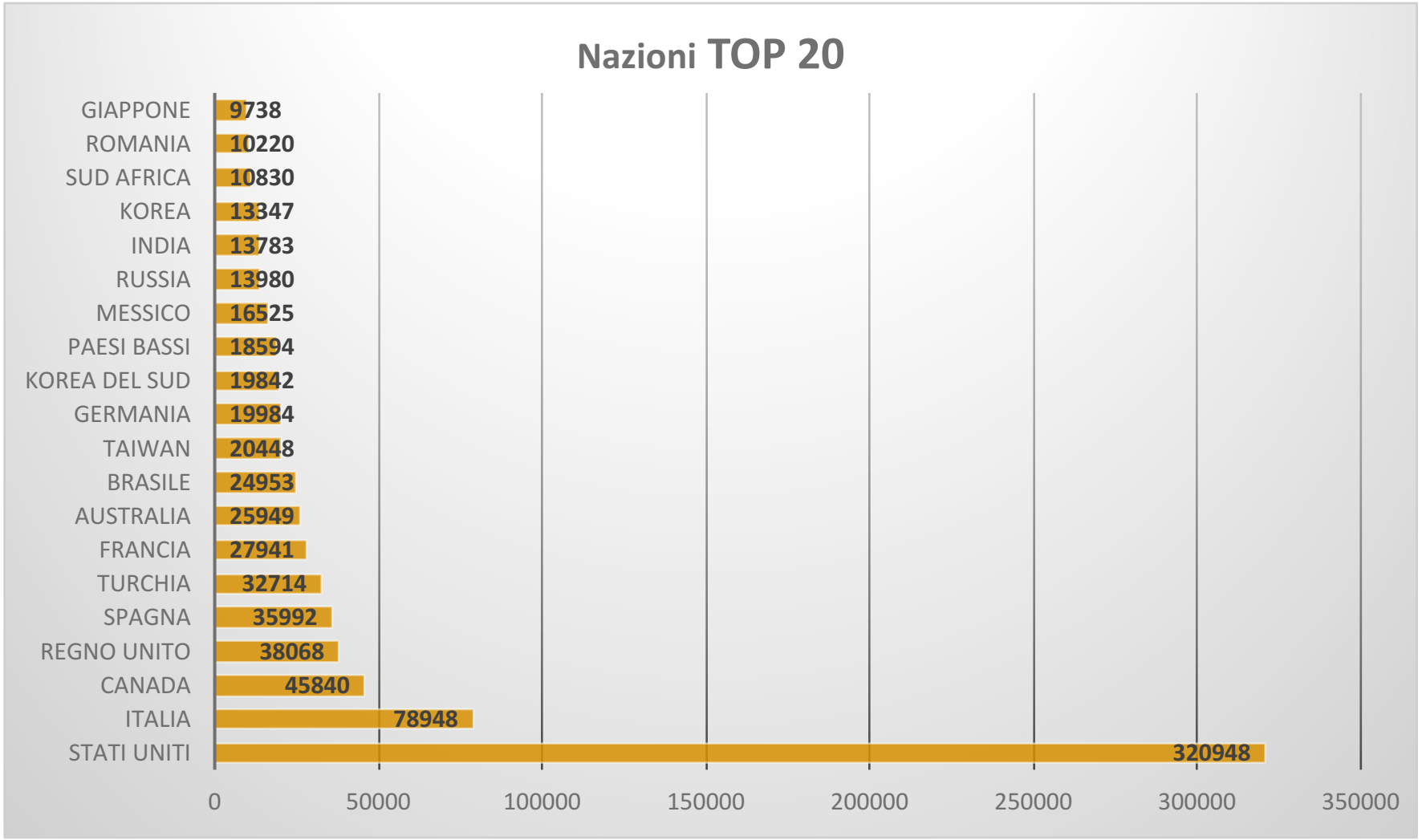
- Encrypt the file extensions of your choice.
- Compatible with all versions of windows.
- Send the unlock password to a https web server.
- Leave a message on the desktop.
- Detection rate 3/35 before crypting - just use some crypting service to make it fully undetectable if you want.

Ransomware as a service



Vittime di ransomware

Top 20 nazioni per diffusione Ransomware*



*studio Microsoft: https://blogs.technet.microsoft.com/mmpc/2016/05/18/the-5ws-and-1h-of-ransomware/

Infezioni BOT EMEA*

Nazioni	Città nell'area EMEA	Città in Italia
1. Turchia	1. Istanbul, Turchia	1. Roma
2. Italia	2. Ankara, Turchia	2. Milano
3. Ungheria	3. Roma, Italia	3. Arezzo
4. Germania	4. Budapest, Ungheria	4. Settimo Milanese
5. Francia	5. Szeged, Ungheria	5. Cagliari
6. Spagna	6. Mosca, Russia	6. Trento
7. Regno Unito	7. Petah Tiqwa, Israele	7. Torino
8. Polonia	8. Madrid, Spagna	8. Firenze
9. Russia	9. Parigi, Francia	9. Bolzano
10. Israele	10. Londra, Regno Unito	10. Modena

**Fonte: Global Intelligent Network Symantec*

Modalità operative e tecniche d’attacco utilizzate

Modalità di diffusione

Email

- Campagne di SPAM
- Mascherati come fatture, avvisi di consegna (es:DHL)
- Notifiche Equitalia
- Allegati direttamente all'email (.**pdf.exe**, .**JS**)
- Link nelle mail

Exploit Kits

- Ospitati su siti compromessi con sfruttamento di exploit/ vulnerabilità in software presenti sulle postazioni (Flash Player, Java, Acrobat Reader)
- Link inviati a mezzo email, social media o malvertisements

Altri Vettori

Veicolati da altri malware (es: Citadel)

SMS e app store (Android)

File colpiti dalla cifratura

Encryption

Cifratura delle principali estensioni:

3fr, accdb, ai, arw, bay, cdr, cer, cr2, crt, crw, dbf, dcr, der, dng, doc, docm, docx, dwg, dxf, dxg, eps, erf, indd, jpe, jpg, kdc, mdb, mdf, mef, mrw, nef, nrw, odb, odm, odp, ods, odt, orf, p12, p7b, p7c, pdd, pef, pem, pfx, ppt, pptm, pptx, psd, pst, ptx, r3d, raf, raw, rtf, rw2, rwl, srf, srw, wb2, wpd, wps, xlk, xls, xlsb, xlsm, xlsx, zip

Ma l'elenco è in continua crescita...

Target di cifratura

- Dischi locali
- USB Storage Device
- Dropbox, OneDrive, GDrive
- Unità di rete mappate con lettera di unità
- Share di rete
- RDP 3389 ?? (Lokmann.key993, variante di Mobef)

Gestione chiavi cifratura

La prima generazione di Ransomware cifrava dopo aver contattato il C&C (Cryptolocker)
La generazioni successive prima cifrano i dati e poi contattano il C&C

- Chiave simmetrica AES128 (.CryptoHasYou. , CuteRansomware, Enigma, Locky)
- Chiave simmetrica AES256 (GhostCrypt , KryptoLocker, TrueCrypter, VenusLocker)
- Chiave simmetrica 3DES (Job Crypter)
- XOR, XOR 255 (ODCODC, Pclock)
- RSA 2048 (CTB-Locker, CryptFIle2)
- AES + RSA 2048 (CryptoFortress, MaktubLocker, NanoLocker)

Protocolli di comunicazione verso i C&C

FAMILY	PROTOCOL	C&C DOMAINS
Dirty Decrypt	HTTP	DGA
CryptoLocker	HTTP	DGA and hardcoded URLs
CryptoWall / CryptoDefense	HTTP and later TOR	Hardcoded URLs
Critroni / CTB Locker	TOR	Hardcoded URLs
TorrentLocker	HTTPS	Hardcoded URL
Cryptographic Locker	HTTP	No-IP / No-DNS, hardcoded

Fermare i Ransomware

Protezione contro i Ransomware

1. **Installare, configurare e gestire appropriatamente una soluzione di sicurezza dell'endpoint su più livelli**
   - **Per la tecnologia SEP questo significa usare IPS, SONAR, Firewall and Insight e SEP 14 , ATP**
   - **Usare Download Insight per** bloccare i files che il parco clienti di Symantec riconosce come malevoli ma per i quali non è ancora stata effettuata un'analisi dai nostri ingegneri
2. **Educazione degli utenti**
   - Per Symantec questo vuole dire **Phishing Readiness Services**
3. **Corretta gestione dei contenuti consegnati via posta, la scansione e il sandboxing degli stessi**
   - **Mail security .cloud + ATP**
4. **Mantenere aggiornati i sistemi operativi e le applicazioni**
   - **Oltre ai web browers e ai relativi plugins,** web application frameworks quali **Wordpress**, e **Joomla** sono target preferiti
5. **Impedire agli utenti l'esecuzione di applicazioni dalle directory temporanee**
   - Per **SEP** usare le politiche di Application and Device Control per prevenire l'esecuzione diretta di codice dalle root e/o dalle subdirectory degli utenti %AppData%
   - Per **SEP** usare le politiche di Application and Device Control per impedire che programmi non consentiti possano accedere a file documentali (per esempio consentire solo a Word di modificare .doc files)
6. **Limitare gli utenti all'accesso a drive mappati – qualora possibile limitare i permessi alla sola lettura**
7. **Dotarsi di una infrastruttura di backup centralizzata non raggiungibile dai Ransomware**

SEP Ransomware Attack Kill Chain

1. Malware Delivery

AVE, IPS,
Download Insight

IPS

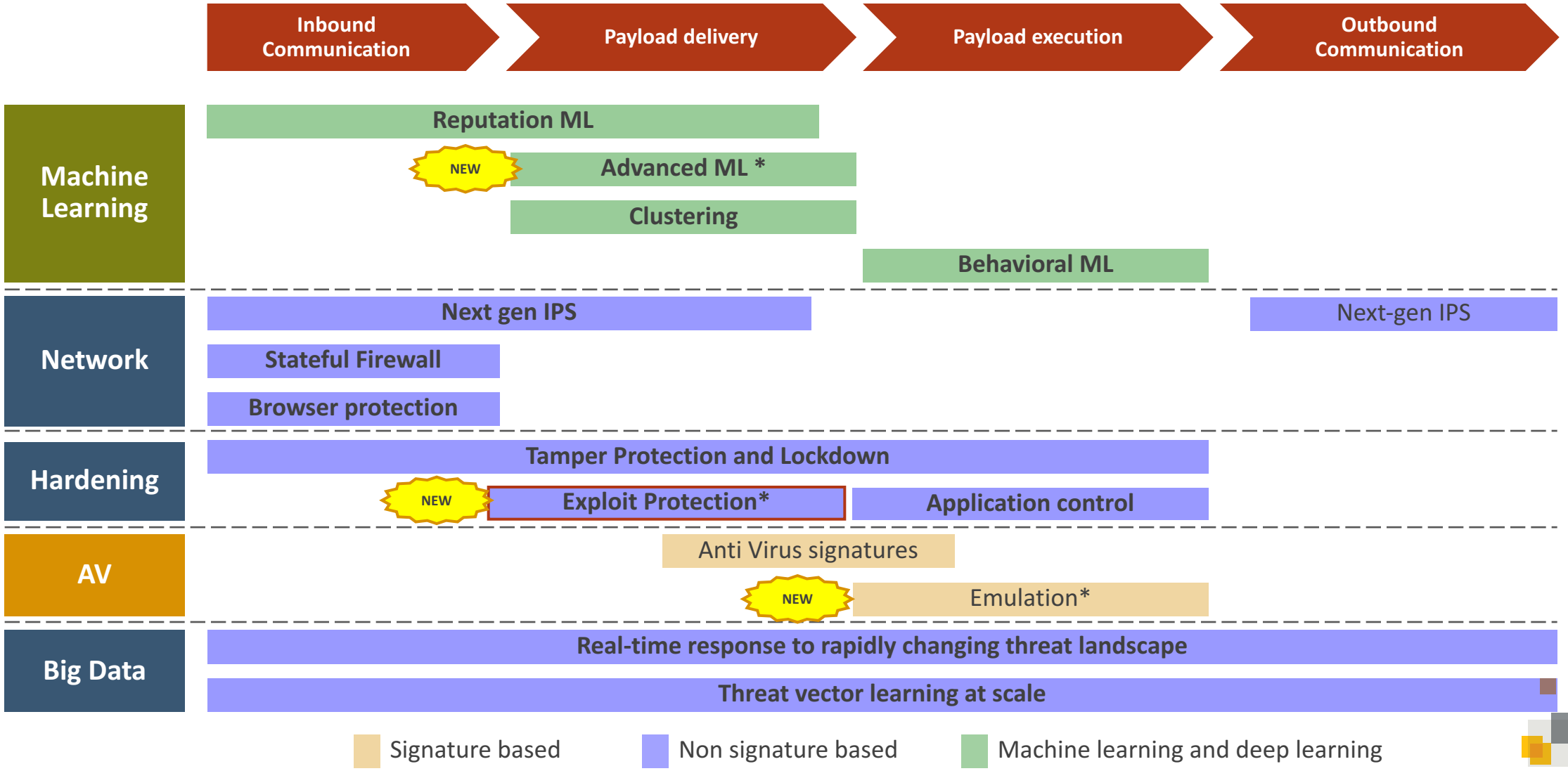
2. Malware installed

SONAR,
A/DC

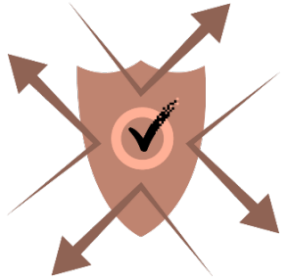
3. Call C&C Server

4. Encryption

SEP 14: Difesa a più livelli



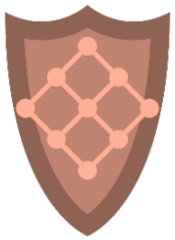
Difesa a più livelli



Prevent Installation

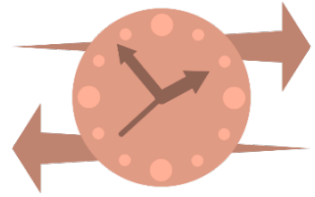
- Email Security
- Gateway Security

- AVE
  - *Heuristics*
  - *Advanced Machine Learning*
- Intrusion Prevention
  - *Browser Protection*
- Download Insight



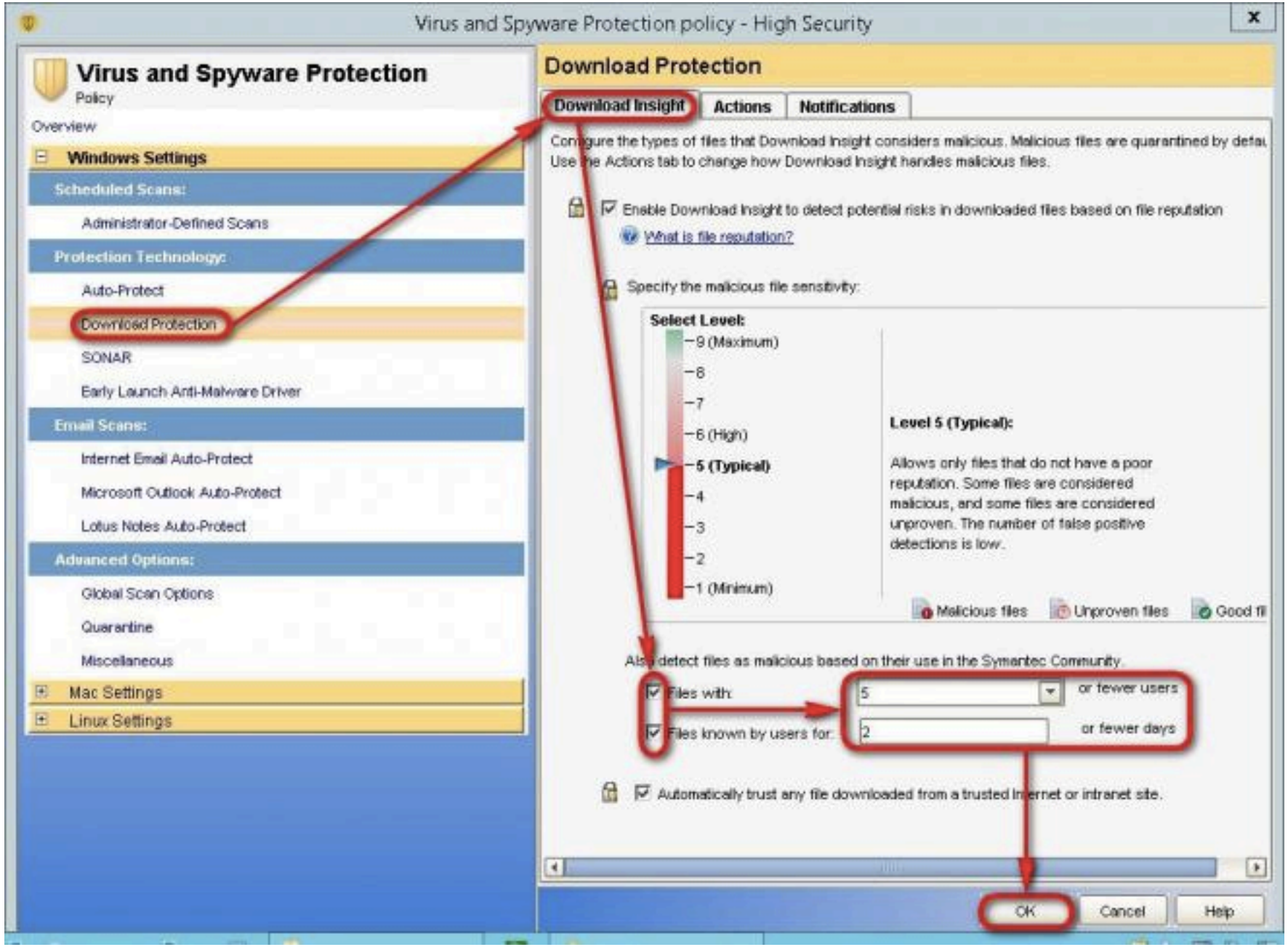
Prevent Encryption

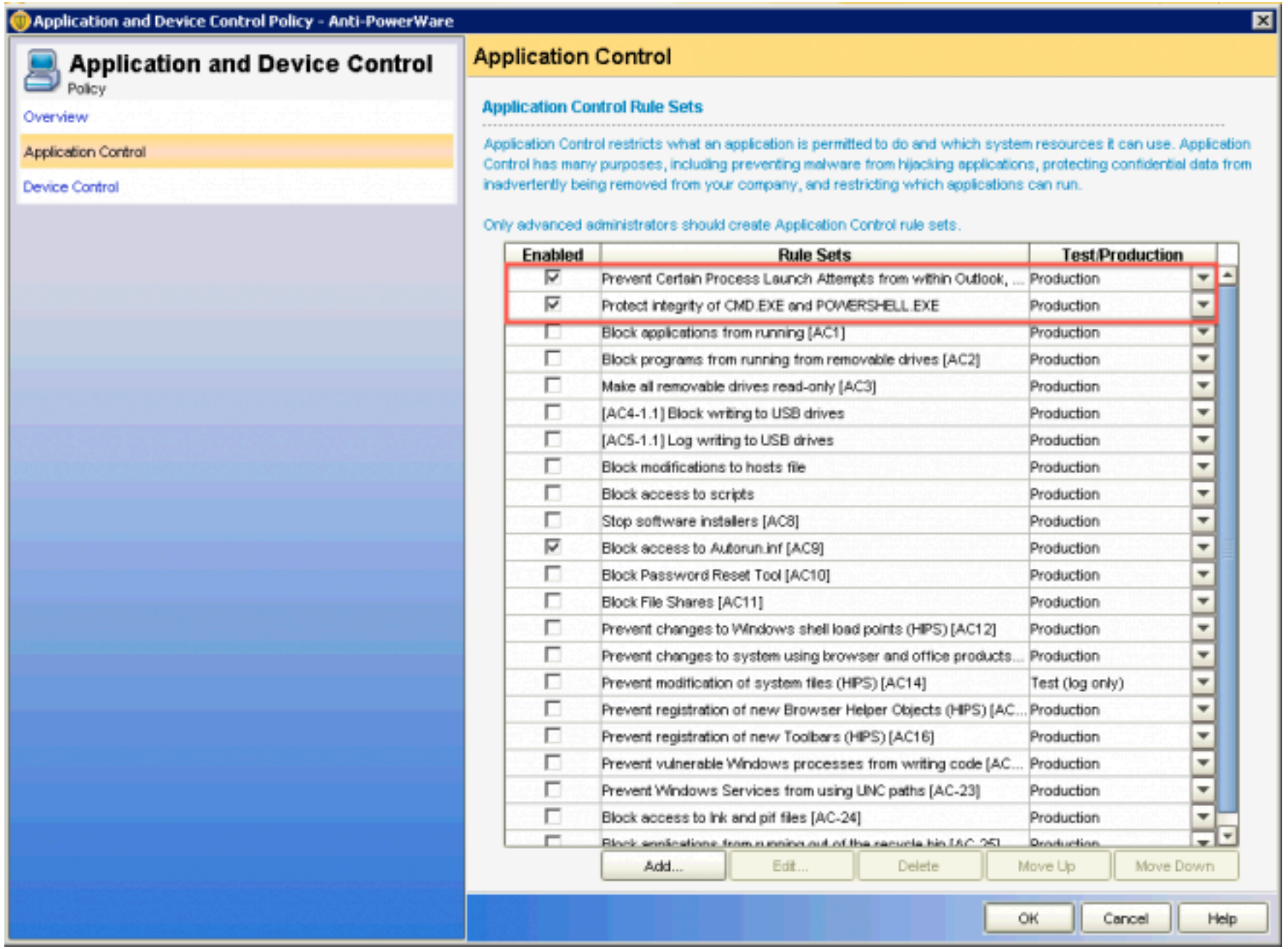
- AVE
- SONAR behavior engine
- Intrusion Prevention
- Application/Device Control

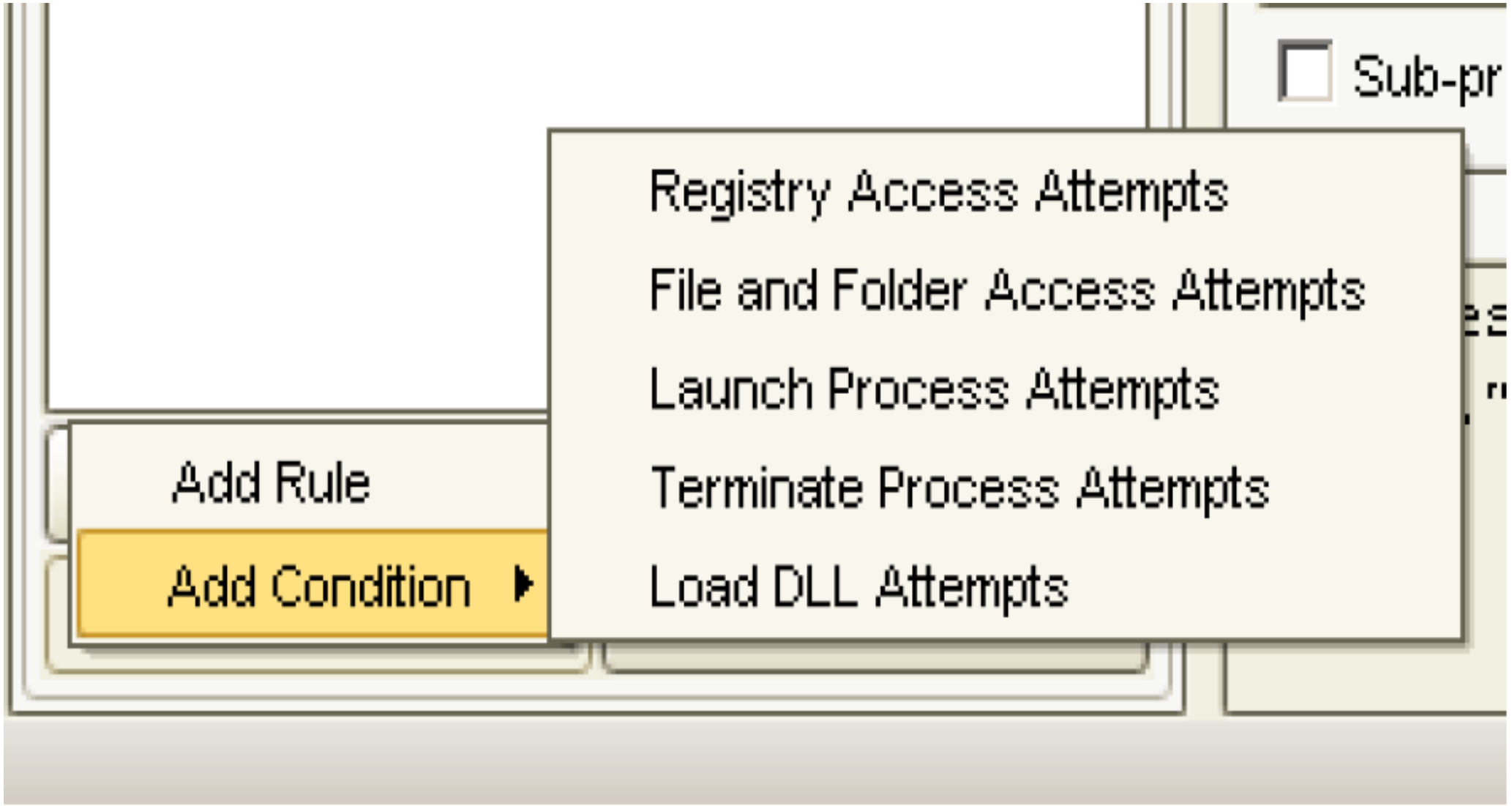


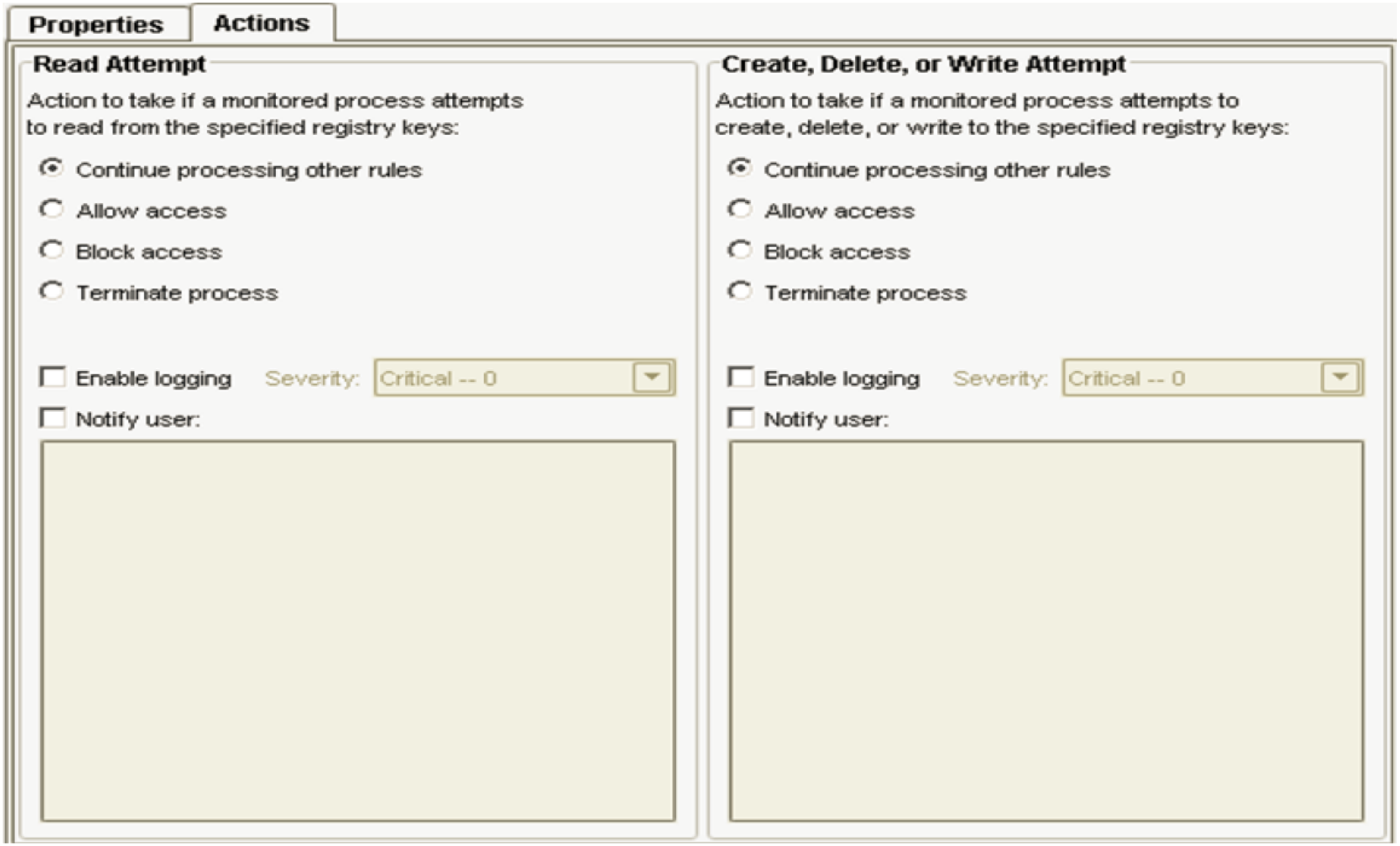
Removal

- File submission to Security Response
- Symantec Power Erase
- Symantec Incident Response Services


Virus and Spyware Protection policy - High Security
Virus and Spyware Protection
Policy
Overview
Windows Settings
Scheduled Scans:
Administrator-Defined Scans
Protection Technology:
Auto-Protect
Download Protection
SONAR
Early Launch Anti-Malware Driver
Email Scans:
Internet Email Auto-Protect
Microsoft Outlook Auto-Protect
Lotus Notes Auto-Protect
Advanced Options:
Global Scan Options
Quarantine
Miscellaneous
Mac Settings
Linux Settings
Download Protection
Download Insight
Actions
Notifications
Configure the types of files that Download Insight considers malicious. Malicious files are quarantined by defau
Use the Actions tab to change how Download Insight handles malicious files.
Enable Download Insight to detect potential risks in downloaded files based on file reputation
What is file reputation?
Specify the malicious file sensitivity:
Select Level:
9 (Maximum)
8
7
6 (High)
5 (Typical)
4
3
2
1 (Minimum)
Level 5 (Typical):
Allows only files that do not have a poor reputation. Some files are considered malicious, and some files are considered unproven. The number of false positive detections is low.
Malicious files
Unproven files
Good fi
Also detect files as malicious based on their use in the Symantec Community
Files with:
5
or fewer users
Files known by users for:
2
or fewer days
Automatically trust any file downloaded from a trusted Internet or intranet site.
OK
Cancel
Help


Application and Device Control Policy - Anti-PowerWare
Application and Device Control
Policy
Overview
Application Control
Device Control
Application Control
Application Control Rule Sets
Application Control restricts what an application is permitted to do and which system resources it can use. Application Control has many purposes, including preventing malware from hijacking applications, protecting confidential data from inadvertently being removed from your company, and restricting which applications can run.
Only advanced administrators should create Application Control rule sets.
Enabled
Rule Sets
Test/Production
Prevent Certain Process Launch Attempts from within Outlook, ... Production
Protect integrity of CMD.EXE and POWERSHELL.EXE Production
Block applications from running [AC1] Production
Block programs from running from removable drives [AC2] Production
Make all removable drives read-only [AC3] Production
[AC4-1.1] Block writing to USB drives Production
[AC5-1.1] Log writing to USB drives Production
Block modifications to hosts file Production
Block access to scripts Production
Stop software installers [AC8] Production
Block access to Autorun.inf [AC9] Production
Block Password Reset Tool [AC10] Production
Block File Shares [AC11] Production
Prevent changes to Windows shell load points (HIPS) [AC12] Production
Prevent changes to system using browser and office products... Production
Prevent modification of system files (HIPS) [AC14] Test (log only)
Prevent registration of new Browser Helper Objects (HIPS) [AC... Production
Prevent registration of new Toolbars (HIPS) [AC16] Production
Prevent vulnerable Windows processes from writing code [AC... Production
Prevent Windows Services from using UNC paths [AC-23] Production
Block access to lnk and pif files [AC-24] Production
Add...
Edit...
Delete
Move Up
Move Down
OK
Cancel
Help


Sub-pr
Registry Access Attempts
File and Folder Access Attempts
Launch Process Attempts
Terminate Process Attempts
Load DLL Attempts
Add Rule
Add Condition


Properties
Actions
Read Attempt
Action to take if a monitored process attempts to read from the specified registry keys:
Continue processing other rules
Allow access
Block access
Terminate process
Enable logging
Severity:
Critical -- 0
Notify user:
Create, Delete, or Write Attempt
Action to take if a monitored process attempts to create, delete, or write to the specified registry keys:
Continue processing other rules
Allow access
Block access
Terminate process
Enable logging
Severity:
Critical -- 0
Notify user:

Symantec Advanced Threat Protection: Moduli

ATP: Network

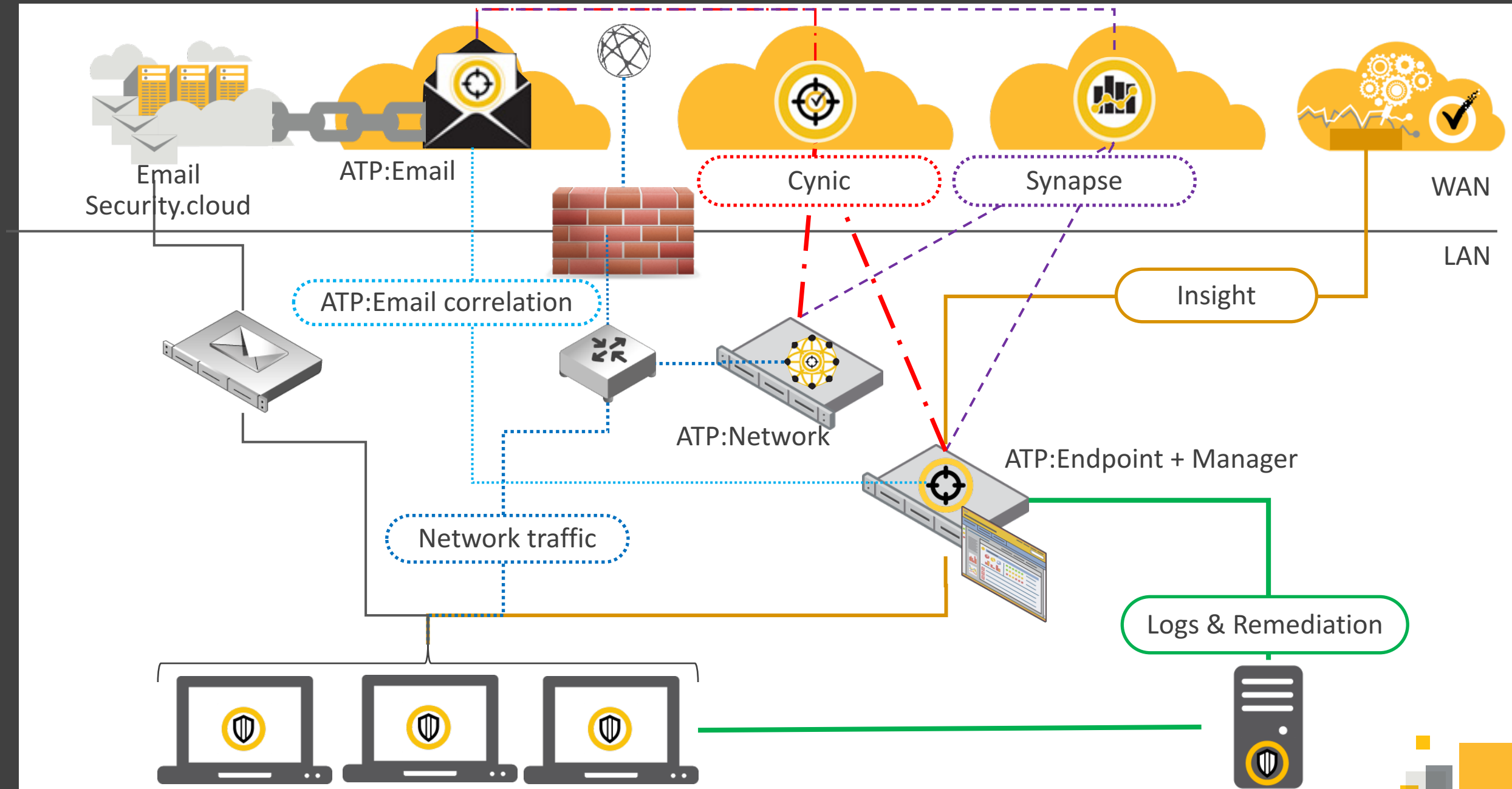
- Visibilità su tutti i dispositivi e protocolli
- Sandboxing, web exploits, command & control automatizzati
- Appliance fisica o virtuale

ATP: Endpoint

- Visibilità sugli endpoint (principale entratura negli attacchi mirati)
- Endpoint context, eventi sospetti & remediation
- Richiede SEP – nessun nuovo agente

ATP: Email

- Visibilità sulla posta (ancora vettore numero uno delle incursioni)
- Email trends, identificazione di attacchi mirati, sandboxing
- Add-on in cloud di Email Security.cloud


Email
Security.cloud
ATP:Email
Cynic
Synapse
WAN
LAN
ATP:Email correlation
Insight
ATP:Network
ATP:Endpoint + Manager
Network traffic
Logs & Remediation

Phishing Readiness

mercoledì 19/10/2016 11:13

Gruppo pagamenti <pagamenti@zx555z.com>

AVVISO NUMERO 091708915680

To Alessandro Ghezzi

Equitalia

Equitalia S.p.A.

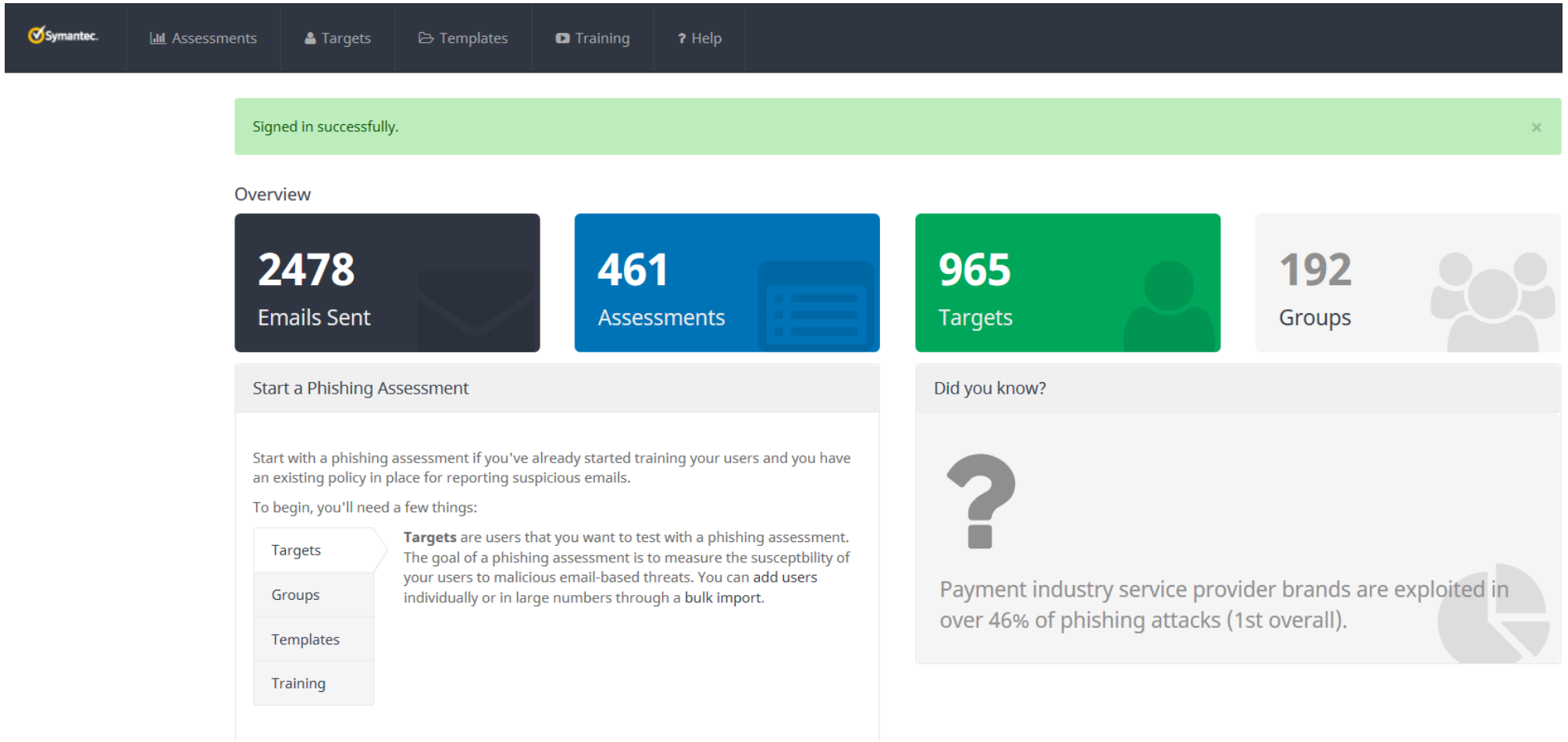
Via Cristoforo Colombo 470 - 0047097 - Roma

Art. 26 D.P.R. 29/09/1973, n. 602 e successive modifiche - Art. 60 D.P.R. 29/09/1973, n. 470, Art. 139 c.p.c

Gentile Alessandro Ghezzi,

Il suindicato Agente della Riscossione avvisa, ai sensi delle intestate disposizioni di legge, d'aver depositato in data odierna, nella Casa Comunale del Comune il seguente avviso di pagamento "**Documento Numero 000793789**" del 01/08/2016, composto da 3 pagine di elenchi contribuenti a nr. 7 atti Scarica il documento

Phishing Readiness



Q&A

Thank you!

Alessandro Ghezzi

alessandro_ghezzi@symantec.com