How to be prepared for the next generation of malware

Martin Zich, CISSP
HPE Pointnext

24th Sep, MS Ignite 2018
Malware
A threat which is here to stay

- Ransomware
- Cryptoware/coin miners – cryptojacking
- Adware
- Banking trojan
- Other malware to steal credentials, PII, and much more.
What we keep finding at our clients
Many disconnected detection controls.

Alerts missing a context.

Inability to detect/react to unknown and take immediate action.

Missing or wrongly trained machine learning.

Lack of visibility.

Lots of unwatched and unpatched current and legacy systems.

Lots of correct “paperwork” which differs from what is deployed.

Lots of victims of social engineering.

User education and training showing dubious outcomes.

Completely paralyzed environments.
We found completely paralyzed companies
We found many victims of social engineering

The were looking for doubtful symptoms like:

**Cryptojacking:**
- CPU/power consumption rise
- Overheating
- Periodical unknown traffic
- etc.

**Ransomware:**
- Usually there was no need to watch for symptoms ... it was too late...
1. Secure hardware base.
Next-generation malware defense
Secure hardware base

- Silicon root of trust with HPE Gen10 – Secure start base
Next-generation malware defense

Secure hardware base for Azure Stack

- HPE ProLiant Gen10 for Azure Stack
  - Silicon root of trust
Next-generation malware defense

2. Locked-down OS platform

- Defending against known “by design“
- Secure configuration (hardening) – CIS benchmarks, STIGs, etc.
Next-generation malware defense

2. Locked-down OS platform

- Defending against known “by design“
- Secure configuration (hardening) – CIS benchmarks, STIGs, etc.

- Microsoft Credential Guard
- Windows Defender Application Control (WDAC)
- Microsoft Device Guard
- Microsoft Edge AppGuard
- Windows S
Next-generation malware defense

3. Blocking the known and blocking the most frequent threat vectors

- At best, right away = without any need for a long analysis
- Defending against specific threat vectors instead of specific threats
- Previously unknown threats included (zero-day)
Next-generation malware defense

3. Blocking the known and blocking the most frequent threat vectors

- At best, right away = without any need for a long analysis
- Defending against specific threat vectors instead of specific threats
- Previously unknown threats included (zero-day)

- Microsoft Exploit Guard
  - Attack Surface Reduction – Office rules, Script rules, Email rule
  - Controlled Folder Access
  - Network protection
  - Exploit Protection
Next-generation malware defense

4. Defending legacy and embedded

- Turning on backported features
- Secure configuration – hardening
- Applications whitelisting
- Network/physical isolation – e.g. separated VLAN for legacy, air-gapped embedded
4. Defending legacy and embedded

- Turning on backported features
- Secure configuration – hardening
- Applications whitelisting
- Network/physical isolation – e.g. separated VLAN for legacy, air-gapped embedded

Microsoft env., for example:

- W8 Restricted Admin mode, backported to Windows 7 (extended support till January 14, 2020).
- Group policies for SLA on e.g. SAM-R (net user, net group, etc.)
- Disabling low-level encryption types (RC4 with NTLM, SSLv1,2, etc.)
- Disabling SMBv1
Next-generation malware defense

5. Detection and stopping the unknown

- Detect and block all of the unknown threat vectors (zero-day)
- Train well the „machine learning“
- Maintaining visibility and taking actions over the whole environment
Next-generation malware defense

5. Detection and stopping the unknown

- Detect and block all of the unknown threat vectors (zero-day)
- Train well the "machine learning"
- Maintaining visibility and taking actions over the whole environment

- MS Intelligent Security Graph + various associated solutions
MICROSOFT INTELLIGENT SECURITY GRAPH

Unique insights, informed by trillions of signals. This signal is leveraged across all of Microsoft’s security services.

- 1.2B devices scanned each month
- Malware data from Windows Defender
- Shared threat data from partners, researchers, and law enforcement worldwide
- 200+ global cloud consumer and Commercial services
- Botnet data from Microsoft Digital Crimes Unit
- 400B emails analyzed
- 750M+ Azure user accounts
- 18+B Bing web pages scanned
- 450B monthly authentications
Intelligent Security Graph

Microsoft feeds its security solutions with information stored and processed in ISG

- **Windows Defender AV** – local ML portion + from-cloud delivered protection
- **Windows Defender Advanced Threat Protection**
- **Office 365 Advanced Threat Protection**
- **Azure Advanced Threat Protection**
- **API** – getting your own context information, security profiles, taking active actions through the API
Intelligent Security Graph – Windows Defender AV

- **Local ML models, behavior-based detection algorithms, generics and heuristics**
- **Metadata-based ML models**
- **Sample analysis-based ML models**
- **Detonation-based ML models**
- **Big data analytics**

**Protection in milliseconds**
- Most common malware are blocked by high-precision detection in Windows Defender AV

**Protection in milliseconds**
- ML-powered cloud rules evaluate suspicious files based on metadata sent by the Windows Defender AV client during query

**Protection in seconds**
- A copy of the suspicious file is uploaded for inspection by multi-class ML classifiers

**Protection in minutes**
- The suspicious file is executed in a sandbox for dynamic analysis by multi-class ML classifiers

**Protection in hours**
- ML models and expert rules correlated signals from a vast network of sensors to automatically classify threats

---

**Cloud-based Protection**

Get Real-time protection when Windows Defender sends info to Microsoft about potential security threats. This feature works best with Automatic sample submission enabled.

- **On**
Intelligent Security Graph – API

Microsoft Graph Security API

Security Providers
- Azure ATP
- Azure AD Identity Protection
- Windows Defender ATP
- Azure Security Center
- Office 365 ATP
- Cloud App Security
- Azure Information Protection
- Intune
- ecosystem Partners

Data and Actions
- Microsoft Graph Security API
- Other Microsoft Graph Services
- Office 365
- Intune
- Active Directory
- More...
- Insights and relationships

Authentication & Authorization
- OAuth 2.0 and OpenID Connect 1.0

Supported SDKs and Sample Code
- .NET
- Xamarin
- WinRT
- JavaScript
- Angular
- PHP
- Android
- iOS
- Ruby
- Python

Getting Started
- GET my profile
- GET my photo
- GET my mail
- GET all the items in my drive
- GET items trending around me
- GET my manager
Intelligent Security Graph – API

Microsoft Graph Security API

Data and Actions
- Alerts
- Security Profiles
- Host | User | File | App | IP
- Actions
- Configurations

Other Microsoft Graph Services
- Office 365
- Intune
- Active Directory

Authentication & Authorization
- OAuth 2.0 and OpenID Connect 1.0

Supported SDKs and Sample Code

Getting Started
- GET my profile
- GET my photo
- GET my mail
- GET all the items in my drive
- GET items trending around me
- GET my manager
Thank You

martin.zich@hpe.com