The Evolution of Cyber Attacks.
And How to Anticipate Malicious Behavior.

Gianluca Busco Arré
Country Manager

Alessandro De Simone
Sales Engineer
State of the Art.

More Attacks, and More Complex.
The 3 Factors of the Bad Guys’ success.

More sophisticated threats, new attack vectors, and greater quantity of offensives.

More complex IT environment with device overpopulation, systems and connections.

Traditional Anti-virus take the same path, but not with such speed.
1. The Attack Evolution.

Malware becomes more and more sophisticated.

Attack techniques are evolving:
The target is not randomly selected, attacks are targeted, coordinated, and use different vectors.

The motive has changed:
From personal recognition to economic gain.
2. Breathe New Digital Life.

Our current digital behavior means a complex, interconnected, and hyper-dynamic environment.

Now, the perimeter is where the user is.

The complexity of IT systems increases vulnerability in the face of cyber-threats.
3. Traditional Protection.

**Based on signature files.**
Their size is getting massive, due to the high volume of malware.

**Only detects known malware.**
As malware gets more sophisticated, companies need to invest more and more time and resources in researching attacks.

**Based on the behavior of old threats.**
These detection systems are obsolete, and only work when known malware gets into the endpoint. They do not monitor activity.

**Offers no information about attacks.**
Due to the increasing complexity of IT infrastructures, the birth of new digital behaviors, and new platforms, traditional protection can’t record the traceability and the effects of attacks.
The Detection Gap.

Time plays a dirty trick on your interests.

18% of new malware remains undetected the first 24 hours, and 2% can even remain undetected for 3 months after infection.

Source: IDG Research, DARK Reading.
Time is Not on Your Side.

Observe how the threat actor is able to compromise a system in minutes or hours, while companies’ reactions usually takes months or even years.

<table>
<thead>
<tr>
<th>From Initial Attack to Initial Compromise</th>
<th>Seconds</th>
<th>Minutes</th>
<th>Hours</th>
<th>Days</th>
<th>Weeks</th>
<th>Months</th>
<th>Years</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7%</td>
<td>16%</td>
<td>54%</td>
<td>10%</td>
<td>10%</td>
<td>2%</td>
<td>2%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>From Initial Compromise to Discovery</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0%</td>
<td>0%</td>
<td>15%</td>
<td>19%</td>
<td>20%</td>
<td>17%</td>
<td>31%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>From Discovery to Containment</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0%</td>
<td>0%</td>
<td>15%</td>
<td>19%</td>
<td>20%</td>
<td>17%</td>
<td>2%</td>
</tr>
</tbody>
</table>

The Target is the Endpoint.

Attackers need to reach the endpoint because from there, they can access other targets, exfiltrate information, steal credentials, gather intelligence, or deploy other attacks.
Hyper-Specialization on Endpoints Activity, User Behavior, and Data Access.

Cybersecurity budgets have been focused on the perimeter, but not on the endpoint.

That’s why, **2-8% of corporate computers are infected** (acc. Gartner).
The Cyber-Kill Chain
The Cyber-Attack's Sequence.

This Cyber-Kill Chain is an excellent tool to understand how organizations can significantly increase the defensibility of their environment by catching and stopping threats at each phase of attacks' lifecycle.
The Situation.

Cyber-crime is a very **attractive and profitable business**.

Attackers count with more and better resources for both technical and economic ones, which allow them to develop even more sophisticated attacks.

The result:

**More and more complex threat dynamics and larger quantity of attacks.**

- **Anyone can deploy an advanced attack.** Thanks to the democratization of the technology, the black market, and the open source tools.

- **All the companies will be an advanced attack’s target.** They should assume it, and start to work in effective security actions and policies.

- **The attackers’ incentive is economic.** They will carry out an offensive just if the attack is profitable; if not, they will give up, to attack another company which can be profitable.
A New Approach to Endpoint Security.

The Ability to Anticipate: A Secret Weapon for Intelligent Cybersecurity.
The Prevailing Paradigm...

... is based on punctual detection only of known malicious processes, this means that:

- All suspicious activity has to be investigated case by case.
- All unknown malicious processes are allowed. That's why attackers skirt around these systems so easily, and their attacks' success rate is so high.

A New Approach to Endpoint Security
A New Cybersecurity Paradigm is Born.

It is based on the classification of absolutely all running processes on your network.

- All activity of all programs is monitored and analyzed in real-time.
- All behaviors are verified by a managed service, the admins don’t have to investigate anything.
- Higher level of protection, fewer efforts, and no risks for you.
It is focused on the intelligent analysis of the behavior of every single process.

As a managed service, analysts and systems “cooperate” together:

- Analysts feed the system.
- The system prioritizes the analysts’ work flow.

100% of running processes are monitored and classified:

- **99.82%** Automatically.
- **0.18%** by Analysts.

Machine Learning allows to reduce the Gap to up to 0.000001.
How to *Fill* the Gap

1st Phase: Comprehensive monitoring of all the actions triggered by processes on hosts

2nd Phase: Analysis and correlation of all actions monitored on customers' systems thanks to Data Mining and Big Data Analytics techniques

3rd Phase: Host hardening & enforcement: Blocking of all suspicious or dangerous processes, with notifications to alert network administrators

**BIG DATA ANALYTICS + HOST ENFORCEMENT**
Phase 1: Monitoring

The host agent monitors all the actions triggered by running processes. Each event is cataloged (based on more than 2,000 characteristics) and sent to the cloud:

- File downloads
- Software installation
- Driver creation
- Communication processes
- DLL loading
- Service creation
- Creation and deletion of files and folders
- Creation and deletion of Registry branches
- Local access to data (over 200 formats)
Phase 2: Big Data Analytics

**Information**
- Static
- Contextual
- External (3rd parties)
- Controlled execution and classification on physical machines

**Classification score**
- The Classification score of each process is recalculated based on the dynamic behavior of the process.
- The Classification scores recalculated based on the new evidence received (Retrospective Analysis).

**Key Figures**
- 27 Years gathering real data from real threats in real environments
- +1B Files have already been categorized over the course of Panda’s history
- +40T 40,000,000,000,000 file attributes
- +500M New files imported daily
- +200M Every day we neutralize more than 200,000 new malware samples
Phase 3: Hardening and Enforcement

The service classifies all executable files with near 100% accuracy (0.000001% of risk). Every process classified as malware is immediately blocked.

Protection against vulnerabilities
The service protects browsers and applications such as Java, Adobe or Microsoft Office against security flaws by using contextual and behavioral-based rules.

Data hardening
Only trusted applications are allowed to access data and sensitive areas of the operating system.

Blocking of all unclassified processes.
All unclassified processes are prevented from running until they are assigned an MCL (Maximum Confidence Level) by the system. If a process is not classified automatically, a security expert will classify it.
The Evolution of the Cyber Attacks

### Malware life cycle on the computer

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Action</th>
<th>Path/URL/Registry Key/IP:Port</th>
<th>File Hash/Registry Value/Protocol-Direction/Description</th>
<th>Trusted</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/9/2016 3:38:03 PM</td>
<td>1</td>
<td>Creates a Registry Key pointing to an exe file</td>
<td>REGISTRY\USERS\S-1-5-21-3286655578-10919891218-20006878754-1004\CLASSES\CLSID{F28C2F70-47DE-4EA5-8F4D-7D1476CD1EFS}LocalServer32?</td>
<td>C:\Documents and Settings\Admin\Mis documentos\Downloads\Neil Armstrong transmision original del alunizaje 1969 Apolo 11.mp4.exe</td>
<td>Unknown</td>
</tr>
<tr>
<td>11/9/2016 3:38:03 PM</td>
<td>1</td>
<td>Creates a Registry Key pointing to an exe file</td>
<td>REGISTRY\USERS\S-1-5-21-3286655578-10919891218-20006878754-1004\CLASSES\CLSID{F28C2F70-47DE-4EA5-8F4D-7D1476CD1EFS}LocalServer32?</td>
<td>C:\Documents and Settings\Admin\Mis documentos\Downloads\Neil Armstrong transmision original del alunizaje 1969 A</td>
<td>Unknown</td>
</tr>
<tr>
<td>11/9/2016 3:38:04 PM</td>
<td>1</td>
<td>Creates a Registry Key pointing to an exe file</td>
<td>REGISTRY\USERS\S-1-5-21-3286655578-10919891218-20006878754-1004\CLASSES\TypeLib{15781A6-3E5C-404A-9118-C1D91FS3704}10.0\0\win32?</td>
<td>C:\Documents and Settings\Admin\Mis documentos\Downloads\Neil Armstrong transmision original del alunizaje 1969 Apolo 11.mp4.exe</td>
<td>Unknown</td>
</tr>
<tr>
<td>11/9/2016 3:38:40 PM</td>
<td>1</td>
<td>Communicates with</td>
<td>127.0.0.1</td>
<td>UDP-Unknow</td>
<td>Unknown</td>
</tr>
<tr>
<td>11/9/2016 3:38:40 PM</td>
<td>1</td>
<td>Communicates with</td>
<td>127.0.0.11630</td>
<td>UDP-Bidirectional</td>
<td>Unknown</td>
</tr>
<tr>
<td>11/9/2016 3:38:48 PM</td>
<td>1</td>
<td>Communicates with</td>
<td>0.0.0</td>
<td>TCP-Unknow</td>
<td>Unknown</td>
</tr>
<tr>
<td>11/9/2016 3:38:48 PM</td>
<td>1</td>
<td>Communicates with</td>
<td>54.6932.59.80</td>
<td>TCP-Bidirectional</td>
<td>Unknown</td>
</tr>
<tr>
<td>11/9/2016 3:38:49 PM</td>
<td>1</td>
<td>Communicates with</td>
<td>198.76.119.80</td>
<td>TCP-Bidirectional</td>
<td>Unknown</td>
</tr>
<tr>
<td>11/9/2016 3:39:52 PM</td>
<td>1</td>
<td>Loads</td>
<td>PROGRAM FILES\MOVIES TOOLBAR\SAFETYX\SAFETYX.CRT.DLL</td>
<td>9994BF035813FE8EB6BC98ECBDB5B0E1</td>
<td>X No</td>
</tr>
<tr>
<td>11/9/2016 3:39:55 PM</td>
<td>1</td>
<td>Runs</td>
<td>TEMP\087B213b8b8\temp\etupesan.exe</td>
<td>F69E31FAA489159ABD590D00DC2CC94A5</td>
<td>X No</td>
</tr>
</tbody>
</table>

The Evolution of the Cyber Attacks
Real Time Monitoring

- The real time monitoring provides the status of all security events, all infrastructure applications behavior (by unit, by division, by country or by groups), along with an analysis of a large set of parameters.
- The company can manage all the parameters, tag machines, define threshold-based alerts (for instance, when a data connection reaches an unusual country, etc).
Application Monitoring

- This information enables Advanced Reporting Tool to automatically generate security intelligence:
  - Find relevant information
  - Diagnose network issues
  - Alert and be alerted
  - Create horizontal and vertical insight
Security Data Usage

- To secure Data you will need full visibility. From file touched, directory created, file actions executed, to exfiltration data analysis. Everything real-time.
- Detect information leaks, both from malware and employees, from any archive that contains data (ex.: pdf, word, excel, txt,...).
Let’s see in action...

Live demo
Reinventing Cybersecurity.