Microsoft

Malware Protection Center

Overview and lifecycle

What is an APT?

Unlike traditional malware infections, advanced persistent threats (APTs) use malicious programs combined with hacking tools and techniques directed at a specific target and with a well-defined motivation.

They are also defined as follows:

- Advanced – they're often hard to detect and use more sophisticated tactics than average malware.
- Persistent – they use a variety of techniques over a long period of time to compromise the target. They are also skilled at evading remediation and mitigation so that they avoid detection.
- Threat – they target and attack specific victims.

The typical feature of an APT that distinguishes it from a malware campaign is that an APT will have a specific target. APTs are also often well funded.

APT attacks can target any level or division of industry and society: they are defined by the fact that they target their attack, often to steal information or cause disruption to the target.

Attacks can be aimed across the spectrum of information users, from home PC users, enterprises, or industries, through to specific, individual companies or persons.

The APT lifecycle

Generally, an APT has the following lifecycle:

1. Intrusion into a specified target and reconnaissance
    a. Commonly via phishing (especially spear-phishing and whaling) or social engineering.
    b. Reconnaissance allows the APT to determine the best way to gain and maintain intrusion.
2. Use of customized exploits
    a. Often serving up exploits that utilize zero-days.
    b. Also using non-zero-day exploits for victims that don't have the latest patches/known vulnerability fixes.
    c. Often combining a collection of multiple exploits for different stages of the attack (for example, remote code execution, privilege escalation, lateral movement).
3. Theft and/or disruption

a. Information is usually stolen and is often the main purpose of APTs – in particular confidential or business-sensitive information.

b. Disruption-focused APTs are almost another category in their own right, as they seek to alter or modify key infrastructure, such as power generation.

c. Valuable assets that facilitate compromise of other targets are also often targeted by APT (for example, stealing a code-signing certificate or a token access code to compromise another target).

4. Maintenance, persistence, and information theft

a. Access is usually maintained via remote access tools (RATs), custom backdoor trojans (utilizing command and control servers), stealth covert channels, and other typical malware-intrusion techniques. The lists of specific vulnerabilities that are targeted are also changed and updated to stay ahead of patches. This ensures persistence on the infected network or machines.

b. Data or information is stolen in a stealthy way, such that the intrusion remains undetected and encourages further persistence.

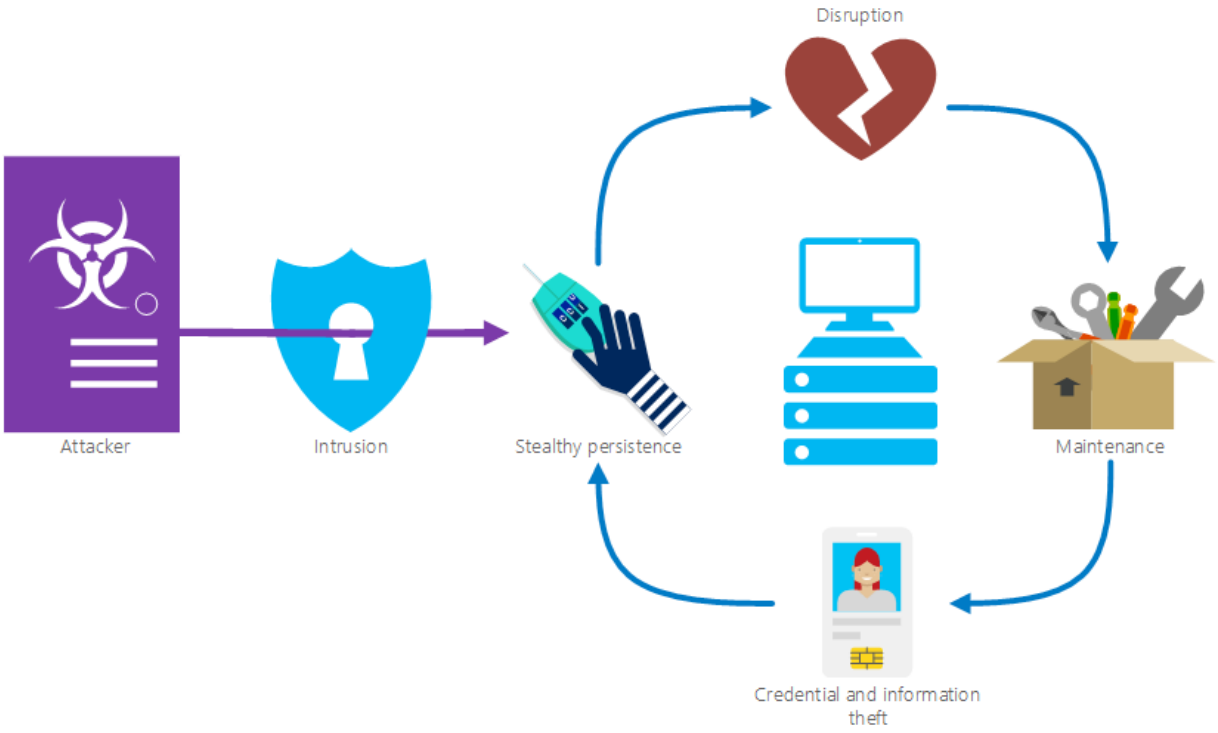

Figure 1: Cycle of an APT: Intrusion, and then continual theft or disruption, maintenance, and persistence






Attack trends

Characteristics

APTs achieved near-household recognition around 2012, following the high profile and well-publicized discoveries of Stuxnet, Flame, and others. However, they've been around far longer (at least since 2005) with campaigns led by what were referred to as "hacking groups" or simply an "adversary". You can read more about these campaigns in our blogs:

- The Stuxnet sting: http://blogs.technet.com/b/mmpc/archive/2010/07/16/the-stuxnet-sting.aspx
- Flame malware collision attack explained: http://blogs.technet.com/b/srd/archive/2012/06/06/more-information-about-the-digital-certificates-used-to-sign-the-flame-malware.aspx

The lifespan of an APT attack can vary widely, and is often in relation to the specificity of the target. An APT that targets a specific company might be short-lived, as it uses high-resolution targeting techniques (such as spear-phishing or whaling) to quickly get into a specific network, steal the information, and then leave.

Alternatively, an APT that is defined by the actor rather than the target may be longer and larger in scope, as it attempts to cast a wide net at the intrusion stage, in the hopes that a small percentage of infections is worth the massive flood.

For example, the APT attack might employ simple social engineering techniques (such as an attractive title on a file that would be of interest to citizens of a specific country or region) but use those techniques in a much larger context (such as distributing the file alongside an illegal download on a global file sharing service).

This method is similar to spam: throw it out to a large context in the knowledge that at least some of the target will be present in that context.

APTs and malware

Individual malware families and customized exploits are often used as part of an APT attack. For example, we saw one vulnerability used in an APT-style attack that appeared to attack a specific population; email attachments used keywords that had been appearing in local news headlines. When opened, the attachments would attempt to exploit the vulnerability on the receiver's machine.

Further examples of APTs and analyses of their methods can be found in the Analysis and statistics section.

Microsoft's efforts

Antimalware research

Microsoft has a strong history of industry-leading research committed to addressing the continuously evolving threat landscape facing our customers.

We invest heavily in research, investigation and analysis of APTs and hire the best researchers and data scientists in their field to advance this work.

Much of the work our researchers and scientists do is related to protecting our users from malware by using the telemetry we receive through the MAPS program in our antimalware clients (such as Windows Defender) that tell us if our remediation and detection is successful.[1] This data and associated protection has a follow-through effect as it impacts on the work we do to track down and determine APT attacks.

For example, as part of a normal customer submission, our analysis might determine that the file could be part of a larger APT attack.

Our dedicated team of APT researchers then use our normal malware analysis techniques, alongside investigative research into the capabilities and characteristics of the file, to determine if it belongs to an existing or new APT attack. This research involves looking at the file in comparison to telemetry we gather, known analysis from the antimalware industry, and analysis against files for which we have existing data.

1 See the Windows 10, Windows 8.1, and System Center 2012 Endpoint Protection privacy statements for more information on the data we collect. For information on enabling MAPS for endpoints running Windows Defender in Windows 10, see https://technet.microsoft.com/en-us/library/mt622088(v=vs.85).aspx.

APT tools and techniques

We observe activities from watering-holes, known command and control server lists, keyword analysis, and known malware behaviors to help us determine the global status of existing and new APTs in the wild.

We also employ other techniques and tools that are specific to further understanding how an APT-related file functions. These techniques include virtual machine detonation or "deep analysis", where we can run and manipulate a suspicious file in a sanitized or "clean" environment. This also allows us to find exploits (including zero-day exploits) that are either being exploited in the wild, or that we have found being targeted in our environment.

The deep analysis environment lets us control everything that the file sees or manipulates (including time and space). After placing the file in this environment and manipulating it, we can determine its purpose based on characteristics and behaviors such as:

- What it does over time
- The APIs it attempts to hook
- The settings or files it tries to modify
- The remote servers it tries to contact

Other tools allow us to determine how the file interacts with other files locally, within the network, or across the Internet.

Analysis and statistics

Multiple industries, similar characteristics

While APTs are largely defined by a similarity either in the actor or the target, generally APT research is focused on threats that target largescale corporations, industries, or other entities such as governments and organizations.

For example, the malware involved in an APT might all use spoofed, customized versions of company-specific log-in portals to steal credentials. The credentials are used for the intrusion aspect of the attack (either by the actor or the "customer"), and the "customer" then has the ability to steal specific information from the target.

Even though the targets vary, the same techniques are used which could indicate that a single APT is behind all of the attacks.

Zero-days and social plays

A common attack vector for APTs is the use of zero-days and targeted social engineering to gain an initial foothold into the target's network, followed by the deployment of specific malware to maintain the infection and steal information.

For example, vulnerabilities (whether zero-day or not) can be used to deliver malware via email attachments aimed at very specific, geographical-based industrial targets. The email attachments could employ standard social engineering techniques that lure users in the targeted organization to unwittingly allow exploitation of the vulnerabilities.

These social engineering techniques could be targeted to a wider group that the final target is a member of. For example, the file names of the attachments might:

- Indicate a specific topic that would only be of interest to the residents of the targeted country or region
- Include references to the country or region itself (or the government of the country or region)
- Be written in a language specific to that country or region

After the initial intrusion, the APT could deploy malware families that steal user credentials and allow for maintenance and persistence on the machine. The malware creates backdoors into the network that allow the attacker to use RATs and command and control servers to remotely access and maintain the intrusion and information theft. The initial malware then deletes itself, further avoiding detection and encouraging persistence.

An ever-widening pool of credentials

STRONTIUM is an example of an actor that we've seen using zero-days to target government-related entities,






including military forces and diplomatic installations. In particular, the actor appears to be targeting NATO member states.

This actor uses publically accessible email lists and forum information to determine individuals it can target for spear-phishing. This can last for a long period – from a month or two to a year or longer.

Once a user's credentials are stolen, the actor can gain access to higher and higher level employees within the organization in ever-escalating credential theft. Eventually, the actor will define the ultimate targets for spear-phishing after building up a picture of the organization from the initial round of theft.

We've seem STRONTIUM infect the target's machine with varying malware, including members of the Foosace family (such as Trojan:Win32/Foosace.C). The malware then allows backdoor access to the actor, who moves laterally throughout the organization, identifying key information for theft.

The STRONTIUM actor exploits a number of vulnerabilities on infected machines. Regular patching and updates (such as Security Bulletins MS15-033 and MS15-070) is vital to preventing attacks from APTs.

The attacks led by STRONTIUM are discussed and analyzed in depth in volume 19 of the Microsoft Security Intelligence Report.

Mitigation and prevention

APT risk mitigation: An ounce of prevention is worth more than a pound of cure

Addressing an APT issue or defending your infrastructure from a potential attack requires unique solutions. It depends on what you carry, what your software security infrastructure has, what your systems do not have, and what you are willing to invest in to protect your intellectual property and other data.

Although there is no one-size-fits-all solution for the current challenges presented by APT, common sense and history tells us all that prevention is better than the cure.

An APT attack typically comes in phases. The mitigation depends on the severity level that it requires in the context of the attack stage when you have discovered it.

It would be wise and mature for any organization to shift left and put a good APT risk management plan in place to get both the infrastructure and resources ready to recognize and fend off an attack.

Identify risks

Most enterprise organizations have a Security Information and Event Management (SIEM) system where they can monitor any unusual network activities. Aside from relying SIEM, first you need to answer these questions to gauge whether your organization is aware of the risks that an APT attack can bring in:

- How much does a typical data breach cost for your enterprise?
- What's the difference between a critical work disruption or a minor data compromise?
- Where do you need to look to discover compromised systems on your network?
- What tools do you use to uncover stealthy attacks?
- Do you know the characteristics of an APT attack?

A good inventory of your assets and your willingness to walk the extra mile to protect those assets will help determine the steps that you can take to address and act on these questions.

Plan risk responses

It pays to get your systems and your human resources ready. That's why smart companies have fire drills - they don't wait for it to happen before telling everyone where the fire escape is. Risk responses can include the following:

- Conduct enterprise software security awareness training, and build awareness about malware infection






prevention.

- Have a good incident response team, if you don't already have one - and a tried-and-tested process to go with it.
- Prepare your software security infrastructure to be forensically ready.

Monitor and control risks

Although APT actors have ways to cover their tracks, there is still a lot that your organization can do to help protect your infrastructure from several channels:

- Ensure your software has the latest patches, update your antimalware signatures, and close the vectors of attack.
- Use application reputation services, such as Microsoft's SmartScreen Filter, to filter the nasties out.
- Use machine learning to help block spam in your network. You can see how Office 365 uses machine learning to help you block spam in the video to the right: First look at Advanced Threat Protection: new tools to stop unknown malware & phishing attacks.
- Reinforce your infrastructure's firewalls, intrusion prevention system (IPS), and intrusion detection system (IDS) to get protection from reconnaissance attacks.
- Use an Enhanced Mitigation Experience Toolkit (EMET) or other exploit protection software to help secure legacy applications.
- Use a comprehensive host- and network-monitoring infrastructure.
- Use SysMon to monitor and analyze command-line instances across the enterprise to find the deployment of indicators of attack related to a suspected APT attack.
- Manage and monitor:
  - Changes to internal DNS servers
  - Code integrity violations of system DLL files (unverified signatures)
  - VPN terminals for anomalous logon activity
  - Kernel crash anomalies of Windows servers
  - Presence of mounted file-systems on servers, discoverable through handles and forensic tools
- Disconnect machines exhibiting compromise characteristics and block command and control URLs if you suspect significant data loss.
- Identify the potentially compromised accounts and begin monitoring for anomalous usage:
  - Reset passwords and/or decommission confirmed affected user accounts
  - Lock down privacy settings on social profiles
  - Restrict remote access to as-needed only






- Isolate local administrator accounts
- Back-up sensitive data

- Educate employees to:
  - Discern suspicious emails and avoid their traps (social engineering, phishing, mal-attachments)
  - Keep personnel and personal data private

Top detections for the past 30 days

The tables in this section show top detections for all malware categories for the past 30 days (not just malware related to APT research). "Distribution" is the percentage share of each detection amongst the top 10 detections in that category.

Enterprise detections	
Threat name	Distribution
BrowserModifier:Win32/Diplugem	20%
SoftwareBundler:Win32/OutBrowse	16%
BrowserModifier:Win32/SupTab	14%
JS/Axpergle	10%
Trojan:Win32/Dorv.A!rfn	8%
Win32/Gamarue	7%
Win32/Sventore	7%
Trojan:Win32/Peals	5%
Trojan:Win32/Skeeyah.A!plock	6%
Trojan:JS/Iframeinject.A	6%

Families	
Threat name	Distribution
HackTool:Win32/AutoKMS	29%
BrowserModifier:Win32/Diplugem	14%
HackTool:Win32/Keygen	11%
BrowserModifier:Win32/Pokki	10%
BrowserModifier:Win32/SupTab	9%
Win32/Gamarue	8%
Win32/Obfuscator	5%
Program:Win32/Hadsruda!bit	5%
Trojan:Win32/Peals	4%
JS/Axpergle	4%

Top detections (all types)	
Threat name	Distribution
HackTool:Win32/AutoKMS	31%
BrowserModifier:Win32/Diplugem	15%
HackTool:Win32/Keygen	12%
BrowserModifier:Win32/Pokki	10%
BrowserModifier:Win32/SupTab	9%
Worm:Win32/Gamarue.gen!lnk	7%
Program:Win32/Hadsruda!bit	5%
SoftwareBundler:Win32/OutBrowse	4%
SoftwareBundler:Win32/Dowadmin	4%
BrowserModifier:Win32/IstartSurf!lnk	3%

Top rogue detections	
Threat name	Distribution
Rogue:JS/FakeCall.D	92%
Rogue:JS/FakeCall.B	3%
Rogue:Win32/Quamatix	1%
Rogue:Win32/Winwebsec	1%
Rogue:MSIL/Rustliver	1%
Rogue:Win32/FakeRean	1%
Rogue:Win32/FakePAV	0%
Rogue:VBS/FakePAV	0%
Rogue:JS/FakeCall.A	0%
Rogue:VBS/Trapwot	0%

Microsoft

Malware Protection Center






Top ransomware detections	
Threat name	Distribution
Ransom:HTML/Crowti.A	34%
Ransom:JS/FakeBsod.A	23%
Ransom:Win32/Crowti	20%
Ransom:JS/Brolo.C	9%
Ransom:Win32/Crowti.A	6%
Ransom:JS/Krypterade.A	3%
Ransom:HTML/Tescrypt.B	2%
Ransom:BAT/Xibow.B	1%
Ransom:Win32/Reveton.V	1%
Ransom:Win32/Tobfy.G	1%

Top exploit detections	
Threat name	Distribution
Exploit:HTML/Axpergle.O	39%
Exploit:JS/Axpergle.BM	20%
Exploit:Win32/CplLnk.A	17%
Exploit:HTML/Meadgive.K	8%
Exploit:HTML/NeutrinoEK.G	5%
Exploit:JS/Axpergle.CB	3%
Exploit:JS/Axpergle.BQ	2%
Exploit:JS/Axpergle.BX	2%
Exploit:HTML/IframeRef.gen	2%
Exploit:Win32/CplLnk.B	1%

Top unwanted software detections	
Threat name	Distribution
BrowserModifier:Win32/Diplugem	26%
BrowserModifier:Win32/Pokki	18%
BrowserModifier:Win32/SupTab	17%
SoftwareBundler:Win32/OutBrowse	7%
SoftwareBundler:Win32/Dowadmin	7%
BrowserModifier:Win32/IstartSurf!lnk	6%
BrowserModifier:Win32/KlipPalCby	5%
BrowserModifier:Win32/KipodToolsCby	4%
SoftwareBundler:Win32/InstallMonetizer	4%
Adware:Win32/EoRezo	4%

Top password stealer detections	
Threat name	Distribution
PWS:HTML/Phish.GK	18%
PWS:Win32/Fareit	16%
PWS:Win32/VB.CU	13%
PWS:Win32/Dyzap.F	12%
PWS:Win32/Prast!rts	11%
PWS:MSIL/Stimilini.M	11%
PWS:Win32/Zbot	7%
PWS:Win32/QQpass.CI	5%
PWS:HTML/Phish.GD	4%
PWS:Win32/Zbot!rfn	3%

Microsoft

Malware Protection Center

Top spyware detections	
Threat name	Distribution
TrojanSpy:Win32/Banker	48%
TrojanSpy:MSIL/Omaneat.B	9%
TrojanSpy:Win32/Banker!rfn	8%
TrojanSpy:MSIL/Hakey.A	8%
TrojanSpy:JS/Phish.D	6%
TrojanSpy:Win32/Mafod!rts	5%
TrojanSpy:Win32/Usteal.D	4%
TrojanSpy:Win32/Ursnif.HN	4%
TrojanSpy:Win32/Banker.XE	4%
TrojanSpy:Win32/Banker.ANX	3%