Resource

- There are more examples of hacking MFA at: https://info.knowbe4.com/webinar-11-ways-to-defeat-2fa.

References

1. 'New exploit hacks LinkedIn 2-factor authentication, with Kevin Mitnick'. YouTube, 5 May 2018. Accessed Aug 2019. www.youtube.com/watch?v=xaOX8DS-Cto.
2. Costas, Paul. 'Is Google To Blame For The Binance Exchange API "Hack"?'. Crypto Disrupt, 12 Mar 2018. Accessed Aug 2019. https://cryptodisrupt.com/is-google-to-blame-for-the-binance-exchange-api-hack/.
3. Erenhouse, Ryan. 'Dispelling the myths: the reality about contactless security'. Mastercard, 17 Jan 2018. Accessed Aug 2019. https://news-room.mastercard.com/2018/01/17/dispelling-the-myths-the-reality-about-contactless-security-2/.
4. Grimes, Roger. 'Smartcard subject hijack hack'. YouTube, 8 Feb 2019. Accessed Aug 2019. www.youtube.com/watch?v=OLQ3lAMuokI&feature=youtu.be.
5. 'Digital Identity Guidelines'. US National Institution of Standards and Technology (NIST), 22 Jun 2017. Accessed Aug 2019. https://pages.nist.gov/800-63-3/.
6. 'Cain & Abel'. Oxid.it. Archived version of site. Accessed Aug 2019. https://web.archive.org/web/20190603235413if_/www.oxid.

Best practices for fighting the fileless threat

Andy Baldin

Andy Baldin, Ivanti

In their continuous quest to find new tools, techniques and tactics to outsmart the white hats, hackers have hit upon a pretty effective strategy. Fileless malware attacks are on the rise, but we still have to worry about file-based approaches, making for a complex situation for defenders.

Recent research has indicated that there were more fileless attack attempts in 2018 than the previous year – and these are just the attacks that have been spotted. Many more are no doubt flying under the radar, helping the bad guys to steal sensitive data, launch ransomware and crypto-mining attacks and much more. The question is, how do IT security teams regain the initiative?

The answer lies with a back-to-basics approach based around some key cyber hygiene processes such as patch management and app control, layered up to maximise prevention and minimise risk. With a good foundation in place, expanding to include detection and response can now be done successfully.

How does it work?

Let's be clear: 'fileless malware' attacks sometimes contain files. In fact, there are a number of different types of attack methodology that fall under this umbrella term. We can divide them up roughly into four distinct areas: malicious documents; malicious scripts; the use of malicious code in memory; and so-called 'living off the land' techniques.

"Fileless attacks that live off the land work by injecting themselves into legitimate applications or processes and using them for malicious ends"

Malicious documents embed scripts or malicious code, allowing attackers to avoid putting executables on disk. Malicious scripts can be executed through web browsers. Malicious code in memory tactics wrap compiled code into scripts that extract into memory – technically still files of a sort except they never get written to disk in order to avoid detection. Finally, fileless attacks that live off the land work by injecting themselves into legitimate applications or processes and using them for malicious ends. As these are normal-looking programs native to the OS they won't show up in Task Manager as being controlled by the malware. What's more, an infection can stay live until a reboot and purge of the fileless malware occurs.

The PowerShell problem

The problem is, there are plenty of programs in Windows that can be manipulated in this way. PowerShell is one of the most commonly used in fileless attacks. This script interpreter runs in system memory and can't be queried, so any malicious activities funnelled through this conduit would be nigh-on impossible to detect. What's more, it has full access to the underlying operating system and is widely used by other Windows programs, meaning that attempts to block it via firewall or AV would be very likely to have a severe impact on the network.

Windows Management Instrumentation (WMI) is another key tool for fileless attackers. Providing access to the targeted machine's registry, it can also perform useful tasks such as switching on WinRM, another native tool designed to remotely execute

PowerShell. Other common Microsoft tools hijacked in these attacks include Visual Basic, Windows UAC Bypass, Windows Registry keys and even the .NET framework.

When it comes to launching the fileless malware, web pages are often used as the delivery mechanism for JavaScript, which in turn could issue commands to PowerShell. Once again, after the commands have been sent, PowerShell can be shut down followed by the web page, leaving no trace of what happened. Other popular delivery mechanisms include Office macros, Flash videos, social engineering and phishing, digital supply chain attacks such as NotPetya, stolen user credentials, malicious Chrome extensions and even in-memory exploits like the infamous EternalBlue, which featured in NotPetya and WannaCry.

Raising the stakes

As you can imagine, given the above variations, there's no typical fileless malware attack. However, there are some examples that can shed light on the tactics sometimes used by hackers. One of the most famous came in 2016 when the state-sponsored entity known as Guccifer 2.0 used these techniques to hack the Democratic National Committee (DNC) ahead of the US presidential election. The subsequent leak of internal Democratic Party emails is widely believed to have swung the election Donald Trump's way, highlighting just how high the stakes can be when it comes to tackling this threat effectively.

"The longer they are allowed to maintain persistence inside a victim's network, the longer attacks have to move laterally, find sensitive data stores and exfiltrate corporate IP and/or customer data"

Given the benefits for the black hats, it's no surprise that fileless malware attacks are on the rise. The Ponemon Institute claimed in 2018 that macros, script, in-memory or remote code execution exploit-based attacks accounted for 30% of all attacks on responding organisations' endpoints in 2017.[1] This rose to 35% the year after and is predicted to comprise 38% of attacks in 2019. Fileless attacks were also ranked second after zero-day threats as "most likely to compromise the organisation" – ahead of file-based attacks and "existing or known attacks".

For IT security teams, it's a race against time to find the right combination of visibility and control to detect and block these techniques. If they stay hidden, attackers can cause significant financial and reputational damage to an organisation. The median dwell time for attackers inside EMEA organisations was 177 days in 2018, more than double the global figure of 78 days. The longer they are allowed to maintain persistence inside a victim's network, the longer attacks have to move laterally, find sensitive data stores and exfiltrate corporate IP and/or customer data. It's no coincidence that breached data is flooding the dark web in ever greater volumes.

Other threats

It's not all about data breaches, of course: fileless attacks are also being used to spread ransomware, crypto-mining malware and other threats, sometimes as part of the same campaign. Industry research claims that crypto-jacking incidents climbed over 400% in 2018. Ransomware may have peaked in terms of infections, but still represents a major threat to organisations, as evidenced by Europol warnings.

Versions such as Sorebrecht have emerged using fileless techniques to bypass traditional filters, in this case abusing Office macros and PowerShell to execute. The authors of the notorious SamSam strain have also used fileless techniques to wreak havoc across the globe, causing $30m in losses to over 200, mainly US-based, organisations, including many hospitals, since 2015. The two Iranians thought to be responsible have been indicted by the US Department of Justice.

The prolific Emotet and Trickbot banking trojans also use PowerShell and macros to infect their victims. The former was detected and removed by one organisation over 1.5m times between January and September 2018, again mainly in the US. Once again, the concern is that as cyber criminals observe the success of these tactics, more will seek to emulate them.

Time for action

Fileless attacks, as we've discussed, aren't often really fileless, and can refer to a range of techniques. The one unifying trait is that they're designed to outwit traditional file-based AV, at a bare minimum. The good news is that this means there are plenty of things IT security practitioners can do to better fortify their organisation against such threats.

The key is to take a defence-in-depth approach. With many different combinations of threat vectors and Windows tools to abuse, it makes sense to layer up protection to stand the best chance of minimising risk.

In practice, this needn't be as burdensome as it might sound. In fact, most of these layers will involve following best practices. Start with patch management, as this helps to reduce the attack surface that fileless malware will look to exploit. Systems should be automated and risk-based to prioritise vulnerabilities currently being exploited in the wild and ensure that all endpoints are covered – no mean feat in an age of digital transformation that has seen an explosion in new networked devices. Combine this with advanced application control to prevent malware and scripts from executing, reducing the number of frameworks that can be used by attackers to covertly execute commands on your systems.

Disabling macros and Flash and preventing PDFs loading in-browser will also reduce your attack surface. Advanced AV tools that use behavioural techniques stand a better chance of spotting the activity associated with fileless attacks. Restricting user privileges and enforcing access controls with two-factor authentication will help to prevent the spread of malware across networks.

Also, don't forget to focus on the 'people' element of security. That means running effective training programmes

to ensure your staff know what a phishing email looks like. Also important from an organisational standpoint is to break down traditional silos that may exist between IT and security operations. It's crucial that any potentially malicious activity spotted by the former is escalated to the latter without delay, and that they are able to pool resources to tackle the threat in the most effective way possible.

This will all take time and potentially a certain amount of extra investment. But as an insurance policy against an increasingly popular black hat trend, it's better to confront the problem head on now than kick it down the road.

About the author

Andy Baldin serves as vice-president EMEA at Ivanti, which provides unified IT and security operations. He has held this position since 2017 and manages Ivanti's EMEA sales team.

Reference

1. '2018 State of Endpoint Security Risk'. Barkly/Ponemon Institute, Oct 2018. Accessed Sep 2019. https://cdn2.hubspot.net/hubfs/468115/whitepapers/state-of-endpoint-security-2018.pdf.

Why do PAM projects fail?

Paul Walker

Paul Walker, One Identity

Every computer operating system and business application needs certain user accounts to function. There's no getting away from that. Accounts with higher levels of permissions (often, but not limited to, administrator accounts) are often referred to as privileged accounts. And these privileged accounts have almost unlimited access across computer systems. As a result, anyone with access to these computer accounts also has access to highly sensitive company information and once these credentials are targeted, they can easily lead to a breach of a company's most valuable assets, from databases to social media and unstructured data.

Most enterprises have implemented some form of privileged access management (PAM) but many find these initiatives fail to live up to expectations. Below are some common reasons why a PAM project might fail to meet the initial expectations coupled with practical insights on how to prevent it from becoming a dud.

Incorrect focus

During PAM project initiation, the must-have business requirements can be overlooked in favour of technical feature sets that could be considered nice-to-have. Some technical features might initially look attractive, although they do not necessarily introduce additional business value.

An example of this is a PAM system that deploys agent-based technology that might seem to offer a greater level of forensic insight and control because it can operate on a lower level than non-agent-based PAM solutions. At the same time, such systems might not be able to cope with an extended scope (such as network devices), and agents are costly to maintain and create additional network traffic. Agents also potentially store sensitive information on the endpoints you want to protect. Agents are more open to being bypassed by privileged users and nearly always introduce deployment delays in the implementation process.

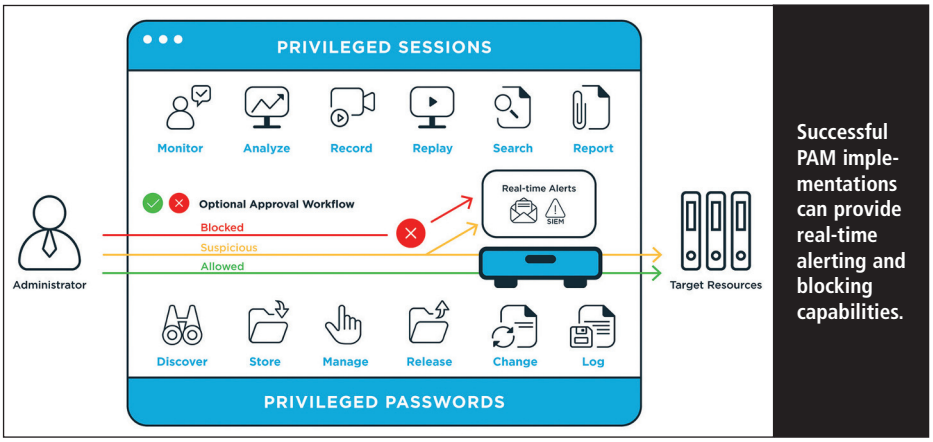
Although it may sound obvious, organisations should focus on the goals of the business. Keeping track of the project's core mission using key performance and risk indicators is often a good way of deciding whether a particular feature or function is relevant to your business. Prioritise the business goals and track or socialise your progress within your organisation to get stakeholder buy-in ahead of technical feature sets. Make sure the organisation will be protected externally as well as from insider threats – and don't forget those perpetrators who steal, misuse or abuse insider accounts to facilitate a data breach.

Think about users

It's also important to think about users, who will include end users, administrators and stakeholders.

End users are the people who perform administrative functions on computer systems and applications as part of their day-to-day job. Their access and what they are doing on these systems need to be subject to security controls – the processes require access to privileged passwords/secrets (such as API keys) as well as sessions that are created.

We hear a lot about frictionless security, what does this really mean and



Successful PAM implementations can provide real-time alerting and blocking capabilities.