being seen as difficult and complicated by many IT professionals. But the reality is that these technologies are only as problematic as you make them.

The lesson here is to implement a good monitoring tool and then reap the rewards of automation, rather than continue to perform a strange interpretive dance that no one understands. Although it may not feel like an easy feat to set up these monitoring and automation technologies, in the long run it will make the lives of IT professionals much better. They can finally focus their efforts on the important stuff, while the background noise is taken care of at last.

About the author

Leon Adato is head geek and technical product marketing manager at SolarWinds, an IT management software provider based in Austin, Texas. Adato boasts more than 25 years of IT experience, including 14 years working with systems management, monitoring and automation solutions for servers, networks and the web. He is also a Microsoft Certified Systems Engineer, Cisco Certified Network Associate and SolarWinds Certified Professional. Prior to his role at SolarWinds, Adato served as a senior monitoring consultant for Cardinal Health.

Fileless attacks: compromising targets without malware

Steve Mansfield-Devine

Steve Mansfield-Devine, editor, *Network Security*

When a computer is compromised, one of the first things a security or forensic specialist will look for is software that shouldn't be there. Many forms of attack involve malicious software, sometimes created specifically for that target. But as Mike Viscuso, co-founder and CTO at Carbon Black, explains in this interview, attackers are increasingly turning to the legitimate software that's already on the machine as a way of achieving their ends.

Attackers used malware because they needed the capabilities it provided – control over the machine and communications with remote servers. But many of those facilities are provided by the operating system itself. On the Windows platform, for example, a hacker can take advantage of Windows Management Instrumentation (WMI), designed to provide system management information in an enterprise environment and PowerShell, a highly flexible system shell and scripting platform. Or a hacker may be able to simply log in remotely.

"We've been seeing a lot of attacks that have no new files enter into the victim's computer," Viscuso explains.[1] "You don't actually need new malicious files or software on the victim's computer. When you arrive on that computer, you already have all the tools at your disposal. We define non-malware attacks as those that are 'living off the land', pure in-memory attacks and other attacks that simply steal credentials or use stolen credentials in order to log in and perform their activity over a remote desktop."

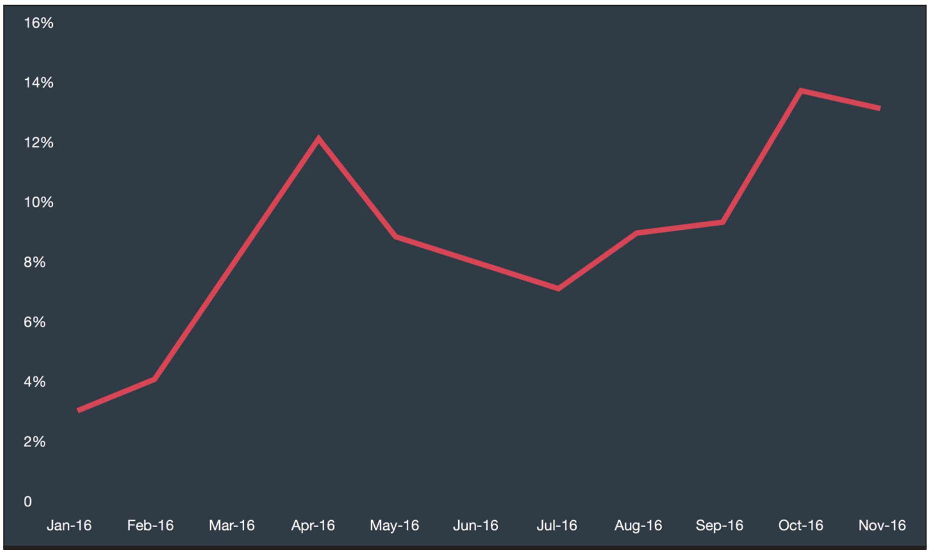
Access paths

The attackers still need to get into the target systems in order to do their dirty work and Viscuso explains that they use the tried-and-trusted methods with which we are all sadly familiar.

"We're talking about software, third-party application vulnerabilities, misconfiguration with the environment," he says. "Just leveraging social engineering via humans. Often we'll see a pure social engineering attack, one where all of the systems are operating exactly as they should be but the human is the weak link. They're actually performing the action on behalf of the attacker."

Malware has become so prevalent that it tends to dominate people's thinking about attacks on computers. There is a great deal of discussion about testing methodologies that focus around malware detection. The message that Viscuso and many others are trying to get across is that malware is not the only threat and that non-malware attacks have been with us for some time – and are on the rise.[2]

"We're asking people to consider, what is an attack and how often does it involve malware," he says. "We did our own study and we saw that 97% of our customers experienced at least one non-malware attack last year. If you look at the trend line of those non-malware attacks, from Q1 to Q4, they increased substantially – so much so, that if you extend that trend line out into Q1 of this year you would expect that one in three organisations would experience a non-malware attack. With so many endpoint products focused on malware – analysing malware, determining whether a new file is malicious or not – these non-malware attacks are far more successful than their malicious counterparts. That has forced a lot of hackers to recognise that these tools have been available for a long time. And they're way more powerful now than they were 10 years ago."



Percentage, by month, of non-malware PowerShell and WMI-based attacks in 2016. Source: Carbon Black.

Switching tactics

One possible scenario is that anti-malware protections have become so successful that attackers are being forced to switched tactics. The vendors of AV products would certainly like you to think so. Viscuso isn't so sure – he suspects the real driver pushing attackers towards non-malware methods is that they are successful, whereas malware-based attacks have a number of hurdles to clear before they can work.

"If you choose to use malware, you'll encounter at least one additional screening – at least one, because if it traverses the network unencrypted it will get sandboxed," he explains. "If it hits the endpoint, it will get evaluated. Sometimes when it's first executed, cloud-based reputation services will say, 'hey we don't know what this thing is' and you'll get reduced privileges when you execute. The reality is that if you just choose not to use malware and use PowerShell instead, you won't go through any of those scrutinies. And so if you're an attacker and it's all the same to you, you can undergo far less scrutiny if you just choose not to use malware. Really the key is that whether you use malware or not is often a choice, not a requirement. I can do the exact same operation with malware or without and in fact I undergo far less scrutiny if choose not to. So, the vast majority of attacks are starting to move that way."

Given that this change of focus has been in progress for some years, why does the security industry still seem so resolutely geared towards malware? Viscuso believes that at least part of the answer lies in the ease with which testing and the sharing of information about malware can be formalised and structured.

"Testing malware is very easy because it can be transferred," he says. "I can send you a hundred malicious samples and it doesn't take an advanced degree in security to know what to do with those samples. You can put them on a test machine, you can run anti-virus, you can execute all 100 or 1,000 of the samples and just see what happens, whereas testing a non-malware attack isn't as easy."

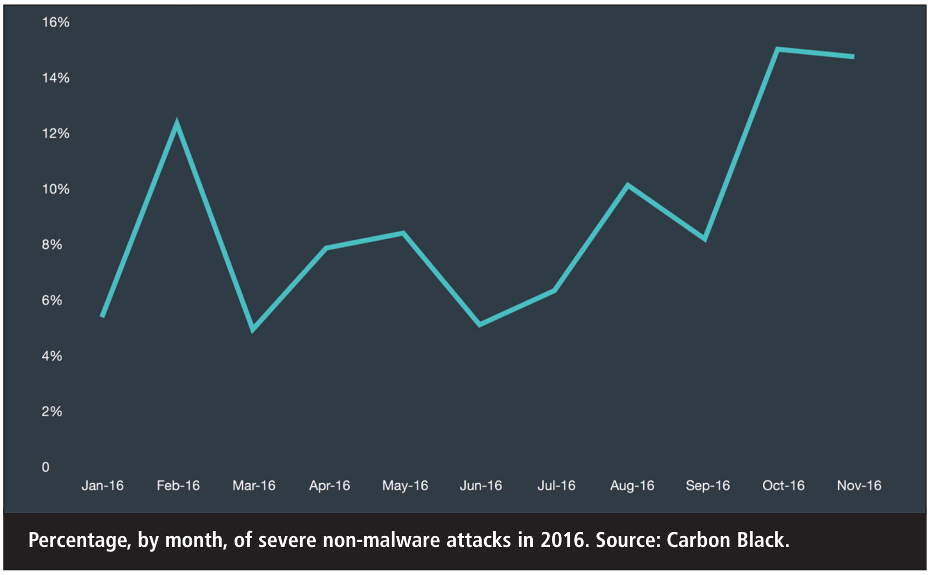
"The key is that whether you use malware or not is often a choice, not a requirement. I can do the exact same operation with malware or without and in fact I undergo far less scrutiny if choose not to"

Non-malware attacks are far more varied and therefore it's harder to create a standardised testing environment. Viscuso points to Metasploit as a key tool that has made testing easier, but also emphasises that it requires relatively high levels of skill and knowledge to employ effectively. And sharing knowledge about non-malware attacks is more complex, partly because of the degree to which you have to understand the environment in which the attack is taking place in order to get the exact same results.

Required skills

As for actually carrying out an attack, one might assume that the non-malware approach might require some inside knowledge about the target, in order to understand the environment and how to exploit it. But Viscuso feels that even where some degree of additional work is required, it's mostly in terms of the kind of reconnaissance that hackers habitually perform. That early stage of a targeted attack hasn't changed much over the years.

"Reconnaissance is the very first step in the kill chain," says Viscuso. "There's manual reconnaissance and there's automated reconnaissance. Automated reconnaissance includes things like scanning for



Percentage, by month, of severe non-malware attacks in 2016. Source: Carbon Black.

open ports and vulnerabilities. Manual reconnaissance is where I'm targeting you – I want to learn about you, I want to go on your website and see what makes you tick." These categories are also broken down into real-time and ahead-of-time activities. "If you imagine I'm trying to send you a PDF that's going to exploit your version of Adobe, I have to hack into that ahead of time," says Viscuso. "But if I'm doing a web-based exploit, I can do that reconnaissance in real time. I can do all of the reconnaissance relating to which version of Java you have, which version of Flash and what plugins you have installed and compare that in real time to the kit that I have and create an exploit specifically for you. So, if you look at the two by two of manual/automated and ahead-of-time/real-time, you can see that there's a variety of different attacks that you could conduct in each of those quadrants."

This is all about getting access to your computer. Once there, though, there are other options as to how the machine can be exploited. A reason for the gradual shift from malware-based to non-malware attacks has been the emergence of powerful tools already installed on the target machines. And one stands out in particular – PowerShell.

"Ten years ago, PowerShell was not a part of the operating system," says Viscuso. "And even in its earlier versions, PowerShell was really just a glorified command shell. Microsoft of course had a big vision for what PowerShell could be and I think we're seeing that vision come through, but really the very first version of the PowerShell was just a different way to interact with the operating system via command shell. Now we've seen the evolution of PowerShell and it's very, very powerful and far more extensible. As an attacker, you didn't really have a whole lot of tools at your disposal 10 years ago – you were forced to create your own malicious software packages. Now, you don't necessarily require an exploit of any sort."

Types of attacker

So who is using this form of attack? Highly targeted attacks involving reconnaissance and carefully tailored social engineering have most commonly been the realm of nation-state (or at least state-backed) attackers. But that's never been exclusively the case and such attacks have become increasingly attractive to ordinary cyber-criminals. So when asked about the users of non-malware attack methods, Viscuso's answer is simple.

"It's everybody," he says. "The reality is that this is a big business. It's been long reported that cybercrime is bigger than the illicit drug business, which also is huge. The reality is that they're just going to do what works. Regardless of whether it's Russia or China or South America, what we're referring to is the tooling necessary to conduct your operation. The tooling goes across all types of threat actors as well as threat motives. The tooling is just a means to an end and the security industry is focused on the tooling."

And that's possibly where we're making our big mistake, reckons Viscuso. As in so many areas of information security the real issue is not one of techniques so much as behaviours. So rather than looking at what files exist on a computer and whether they can be recognised as being malicious, we should be casting our attention to what's happening on the machine in a broader sense.

"We should look at the activity on the computer, not necessarily any one particular file," says Viscuso. "We need to look at the activity across the entire computer and say, does this resemble malicious activity? We don't really care if it's PowerShell or it's some file we don't know about, it's the activity that is indicative of malicious intent."

Michael Viscuso, Carbon Black

Michael Viscuso drives the development of Carbon Black's long-term company and product strategy. He was cofounder and chief executive officer of Carbon Black, which merged with Bit9 in February 2014. A business-minded technologist, Viscuso cofounded Carbon Black in 2011 to provide organisations with protection, detection and incident response capabilities. He has a bachelor's degrees in mathematics and computer science from Villanova University.

Bad behaviour

Anti-malware vendors talk a lot about heuristics and behavioural analysis, which is supposed to make up for the failings of signature-based anti-virus tools. Behavioural Host Intrusion Prevention (BHIPS) is touted as the best way to combat previously unseen threats for which there is no available signature. But Viscuso has his own favourite story about how easy such systems are to defeat.

"When I was creating my own tools and doing my own vulnerability research and exploit development, I had a tool set and every time an AV vendor came up with a new version I had to test my tool set against it," he says. At one point, McAfee was reckoned to have one of the best BHIPS products on the market and indeed it was catching some of Viscuso's tools. In particular, it was detecting when cmd.exe was being launched with the standard input, output and error streams (STDIN, STDOUT and STDERR) directed to a socket – a classic way of gaining a reverse shell. "Well we simply copied cmd.exe to cmd_.exe and did the exact same thing and it worked."

The lesson here, says Viscuso, is that the behavioural features of anti-malware products are an attempt to step up their game from a purely signature-based approach, but they remain inflexible and tend to be focused on a single point in time, such as when a process is first launched: "What that means is that, just like signatures, it's rule based," he says.

In addition, anti-malware systems on endpoints tend to be conservative about behavioural analysis. And they have to be because, as Viscuso puts it:

Attacking DNS

Security researchers recently uncovered an example of a fileless attack that exploited several pieces of legitimate software on the targets' computers. Victims were sent Word documents as email attachments. These contained Visual Basic for Applications (VBA) macros that would launch PowerShell – the first steps in a multi-stage attack exploiting several invocations of VBA scripts and PowerShell instances that led ultimately to the installation of a remote access trojan (RAT).

One of the notable features of the attack is that it used DNS TXT record queries as a bidirectional communications channel with a command and control server. DNS packets are often subject to less scrutiny than other network traffic and may be allowed through firewalls and intrusion detection systems without hindrance.

Throughout the entire process, no files were written to the file system, which allowed the attack to evade most, if not all, anti-malware programs.

There's more information here: http://bit.ly/2oR8KcH.

"Endpoint computers are the wild, wild west. People do all sorts of crazy stuff on the endpoint that is not malicious but you would look at it and think, oh my goodness this has got to be bad. Talk to any instant responder and they'll tell you it is a mess. In tracking down the adversary, you end up tracking down, say, HP more than you track down the most recent Chinese malware variant."

Again, the problems stem from responding to activities at just a single point in time. "It doesn't give you the context you need to be aggressive yet still have low false positives," says Viscuso.

Event sharing

This has led to the development of a different approach, one with its roots in financial services. It's called event sharing and it came to prominence as a result of the emergence of algorithmic or high-frequency trading.

A simplistic method of trading is to impose some basic 'trigger' rules – for example, if a given stock goes below $25 you buy and if it goes above $40 you sell. However, that crude approach is subject to all kinds of problems. For example, if the whole market is falling then just because a given stock is below the trigger point doesn't necessarily make it a good deal. The price of each stock needs to be put in context and so financial firms participating in algorithmic trading began to pull in data from across the markets as well as peripheral information that might have relevance – news sources, weather patterns and even social media feeds. And the firms that were most successful in doing this were the ones that could put all this together and compute decisions faster than the others.

"They pioneered the event-sharing process," says Viscuso. Now that technique is coming to information security. It's an approach that exploits big data in a way that offers context to events to determine whether they represent good or bad activity.

"You can't rely on just a single point in time, such as when a command shell launches and is rerouting its standard in, standard out and standard error to a socket," says Viscuso. "You need to look at it in context. Maybe if a browser that loaded a vulnerable version of Flash was starting this command shell, then that's indicative of malicious software. But the NAC [Network Access Control] client that we use in our company actually does exactly this. It starts a command shell and binds its standard in, standard out and standard error to a local port which it then uses to be able to instruct the command shell to do things and get the results very easily. So you can't just look at one specific point in time, you have to look at the context around that event and constantly update and ask – rather like the high-frequency trading guys – if this is a good thing."

Streaming prevention

Carbon Black calls its approach to this context-aware decision-making 'streaming prevention'. It works by capturing information from endpoints but aggregating and analysing it in the cloud.

"The endpoint is always the destination," says Viscuso, "because it gives you the most flexibility. You can pretty much do anything you want once you have access to the endpoint. You can access data or people, you can manipulate the way that the business works. You can use it to move laterally if you find different fertile ground. So being on the endpoint gives a streaming prevention solution a perspective in being able to record the attacker from the very first step. From very first infection it's able to record the data and as the attacker moves through the computer, or throughout the network, it has a visibility that network-based counterparts aren't able to get."

> ***"You can't just look at one specific point in time, you have to look at the context around that event and constantly update and ask if this is a good thing"***

However, the endpoint is also a noisy place. Factors such as different versions of software running from different locations by different users all add to the complexity. The streaming prevention approach tags events – for example, to identify that, "this is a browser, this is accessing the network, this is accessing the Internet, this is a vulnerable version of this product, this is a shell, this is running a suspended process," as Viscuso explains. "And as we see new attacks we add new tags."

Over the past two years, Black Carbon has added around 200 tags. When examining an organisation's systems, the solution can not only identify the appearance of those identified events, but also reveal the sequencing of them as well as clusters of events. At that point, machine learning enters the picture as part of the enforcement engine that decides if those sequences or clusters represent suspicious behaviour.

"This happens in a loop," says Viscuso. "We're capturing data, tagging it, analysing and deciding; capturing data, tagging it, analysing it and deciding. It keeps happening over and over. As an attacker goes from stage one to stage two, maybe we're suspicious but we're not really ready to say definitively that this is malicious. When it comes back around and we tag the next thing, we do our analysis – not just on that tag like a point-in-time prevention system such as BHIPs would – but we look at that tag and all the tags that came before it and at some point we say, hey you know what, this event sort of pushes us over the edge so to speak: because of that context we feel very comfortable that this is an attack and then we stop it."

Originally, all of the prevention or enforcement part of the operation was cloud-based. The software on each endpoint pushed data up to the cloud systems for analysis and tagging. This provided the system with an enormous amount of data to work with – Viscuso estimates that around 10 million endpoints are working with the solution now.

The solution has evolved, however, and the cloud system is able to push models based on sequences and clusters to the endpoints so that they can operate autonomously to a degree. "The endpoints don't actually need to figure out what an attack looks likes," explains Viscuso. "The cloud tells the endpoint, 'okay when you see something that looks like this, that's an attack you need to prevent'."

This dual cloud/endpoint model has two key advantages, claims Viscuso. "The first is that it allows us to have low false positive prevention," he says. "From the prevention side we're really focused on low false positives: we don't want them getting in the way. But we don't want to miss a big attack and so we actually have our detection in the cloud tuned to be low false negative."

The upshot of this is that the cloud-based system is not only stopping attacks automatically, it is also flagging suspicious activity that hasn't yet gone far enough to warrant automatic enforcement. These suspicions can be shared with the client companies, particularly those running Security Operations Centre (SOCs) where specialists can use this information to make their own decisions. The end result, claims Viscuso, is that the endpoint-based part of the formula provides automated prevention with low false positives while the cloud-based component provides for low false negative detection.

The fact that all the heavy lifting, in terms of machine learning and big data analysis, is done in the cloud means that there's quite a light touch on the endpoint devices.

"A lot of times we'll use far less CPU, memory and disk I/O than the current generation of anti-virus," says Viscuso, "but we will use more bandwidth. And that's connected to the concept of the visibility and context you get by us recording all the endpoint activity. When we do prevent something, you can go all the way back in the chain to the very first action that that attacker took, to identify that root cause, to be able to know which things you need to patch."

"When we do prevent something, you can go all the way back in the chain to the very first action that that attacker took, to identify that root cause, to be able to know which things you need to patch"

Collating all the endpoint data means that this solution can help organisations in other ways, too. Any large organisation will have an IT estate with a large number of vulnerabilities. But which ones represent real threats? Which ones do you need to fix now and which can be left until later? "We can say definitively this is being exploited in the wild," says Viscuso, "because we've actually seen it be exploited in the wild."

Catching zero days

On the face of it, a prevention system that is based on behaviour rather than recognising malicious files sounds like it should be effective against zero-day attacks. Viscuso wasn't keen to commit one way or the other on that score, partly because the term 'zero day' is interpreted in so many different ways by different people. And the term certainly has less direct relevance in non-malware attacks where technique plays a bigger role than technology.

That said, he did relate one interesting tale. "The vendor is still working on solving this, so I can't tell you who the company is, but it's on the top 10 list of most deployed software on Windows," he says. The firm had its code-signing certificate stolen. It got a new certificate but that too was stolen within 24 hours.

Like many software vendors, this firm used automatic updating for its products. Its software would simply reach out across the Internet and download new versions and patches. This updating mechanism was being exploited by criminals as a means of distributing malware.

Carbon Black's streaming prevention system detected that PowerShell was being fired up by the vendor's auto-updating code. That in itself is not unusual. Many vendors employ PowerShell specifically for this purpose. But by monitoring precisely how PowerShell was operating in this case, Carbon Black was able to identify the activity as malicious because of a confluence of events. "This specific instance of PowerShell from this specific vendor was not performing like an auto updater," says Viscuso.

"When this story breaks and everyone is aware of this because the vendor has solved it, I think a lot of people will look back and say, oh my goodness, this could have been hundreds of millions of endpoints compromised if we hadn't found it that early."

About the author

Steve Mansfield-Devine is a freelance journalist specialising in information security. He is the editor of Network Security *and its sister publication* Computer Fraud & Security. *He also blogs and podcasts about infosecurity issues at Contrarisk.com.*

References

1. 'Carbon Black Threat Report: Non-malware attacks and ransomware take centre stage in 2016'. Carbon Black, 15 Dec 2016. Accessed Mar 2017. www.carbonblack.com/2016/12/15/carbon-black-threat-report-non-malware-attacks-ransomware-take-centre-stage-2016/.
2. Viscuso, Michael. 'what is a non-malware (or fileless) attack?'. Carbon Black, 10 Feb 2017. Accessed Apr 2017. www.carbonblack.com/2017/02/10/non-malware-fileless-attack/.