

2017 Malware Trends in Review



Table of Contents

3	Introduction
6	Trend #1: Clickless infection
9	Trend #2: Living off the land
12	Trend #3: Worm capabilities
15	Example attack #1: WannaCry
16	Example attack #2: NotPetya
17	Example attack #3: Emotet

Introduction:




Malware isn't made in a vacuum

It's impossible to discuss malware trends in 2017 without acknowledging the two major outbreaks that dominated the summer. But for all the (well-warranted) attention generated by WannaCry and NotPetya, it's important to keep in mind these attacks didn't come out of nowhere.

Changes in the malware ecosystem are constantly driving and being driven by new adaptations, and in many ways these attacks were natural progressions of trends that have been developing for some time.

Our goal in this report is to paint a bigger picture of how malware has evolved in 2017, and a good place to start is by honing in on the specific elements that made these two year-defining attacks so successful. From there, we can step back and map out the early development and wider adoption of these elements throughout the year.

In doing so, we can see that three key trends emerge:

-  A rise in **clickless infection** driven primarily by the use of remote execution exploits (like EternalBlue) and RDP brute force attacks.
-  The increased practice of **living off the land** — avoiding detection by abusing legitimate system tools and processes rather than dropping malicious files on disk.
-  The resurgence of **worm capabilities** designed to help infections spread further, faster.

Heading into 2018, companies need to be prepared to encounter and protect themselves from these dangerous trends with increasing frequency. To help, this report will provide deep dives into each trend along with recommendations for what you can do now to keep your organization secure.

2017 Malware Trends Timeline

It's not uncommon for advanced tools and techniques developed by targeted attack groups to eventually find their way downstream. Once in the hands of average cyber criminals, they typically get adapted for more widespread campaigns. But this year, that process was accelerated when the Shadows Brokers hacking group leaked a collection of exploits purportedly developed by the NSA, setting the stage for all the attacks that would later utilize them.

By packaging two of these leaked exploits (EternalBlue and DoublePulsar) together with a worm component, the attackers behind WannaCry were able to revamp what had previously been an unsuccessful, run-of-the-mill ransomware variant and launch the largest ransomware outbreak of all time.

A month later, NotPetya built on WannaCry's success, combining the use of EternalBlue with the abuse of otherwise legitimate system tools PsExec and WMIC, enabling the malware to spread deeper inside infected networks, even if devices were patched. Clearly noticing these attacks were onto something, it wasn't long before several banking trojans and other ransomware variants were seen adding similar worm capabilities and techniques, as well.

Throughout 2017, we've also seen increased focus on using Remote Desktop Protocol (RDP) as an infection vector and subsequent path for spreading malware. These attacks typically involve brute-force attempts to crack weak passwords to gain access to remote devices.

By leveraging various combinations of these tactics, attackers are creating infections that are more difficult to block, detect, and contain.

2017 Malware Trends Timeline



JANUARY

RDP attacks spreading CrySIS ransomware increase 2x

FEBRUARY

First WannaCry variant described as run-of-the-mill

MARCH

Microsoft releases security update MS17-010, patching vulnerability CVE-2017-0144 (EternalBlue)



APRIL

Shadow Brokers leak EternalBlue and other NSA exploits

AES-NI ransomware claims to be utilizing EternalBlue

Adylkuzz cryptocurrency mining malware utilizes EternalBlue



MAY

WannaCry utilizes EternalBlue and worm capabilities to infect 400,000 computers

QakBot banking trojan triggers mass Active Directory lockouts with modified worm capabilities



JUNE

NotPetya utilizes EternalBlue and system tools to spread

Sorebrect ransomware mimics NotPetya's use of PsExec for lateral movement

Spike in SamSam ransomware attacks utilizing RDP to spread



JULY

Emotet banking trojan adds worm capabilities

TrickBot banking trojan adds worm capabilities

AUGUST

Eternal Blues scanner identifies 166,000 hosts vulnerable to EternalBlue

Rapid7 scan identifies over 4 million exposed RDP endpoints



CLICKLESS INFECTION



LIVING OFF THE LAND



WORM CAPABILITIES

TREND #1:

Clickless infection



What we're seeing

A growing number of attacks that don't rely on tricking users to launch successful infections.

Why it's happening

The release and proven effectiveness of the EternalBlue exploit has played a big part, but bypassing users also simply allows attackers to infect machines more directly and reduce their chances of detection.

Examples

Attacks leveraging the EternalBlue exploit (WannaCry, NotPetya); RDP brute force attacks (SamSam, CrySiS, Shade, BTCWare).

What's next

Be on the lookout for more WannaCry-like attacks, this time utilizing RDP brute force attacks or exploiting other vulnerabilities.

What to do now

Secure SMB and RDP, patch what you can and isolate what you can't, and deploy endpoint security with exploit and behavioral-based protection.

Deeper dive

End users have long been blamed as the weakest link in security. But many of the latest attacks are bypassing user interaction altogether.

When most of us think of malware delivery methods the obvious ones that jump to mind are malicious emails and exploit kits. Both have long track records of success and both are centered around taking advantage of arguably the most easily exploitable target in any network — the end user.

But this year, many attacks — including the two biggest — haven't involved trying to trick users into downloading malicious email attachments or visiting a compromised website. In fact, they've actually been bypassing user interaction altogether.

The [WannaCry outbreak](#) is a perfect example. In that case, attackers exploited security vulnerabilities in Microsoft's Server Message Block (SMB), a network file sharing protocol, to gain remote code execution on victim machines and launch the ransomware directly. No tricking users with fake invoice attachments or other malware disguises necessary.

The exploit used in the attack, EternalBlue, was one of the purported [NSA exploits leaked in April](#) by the Shadow Brokers hacking group. The good news is [Microsoft update MS17-010](#) addresses the vulnerability and renders the exploit ineffective. Underscoring the severity of the issue, the company also took the unusual step of releasing [updates for older operating systems that are no longer officially supported](#), such as Windows XP, Windows 8, and Windows Server 2003. The bad news is the former update had been available for two months prior to the WannaCry outbreak — a stark reminder of how unrealistic it is to assume that a patch spells the end of an exploit.

Two thirds of ransomware infections in Q1 2017 were delivered via RDP.

— Webroot

But while the spotlight is currently on securing SMB thanks to WannaCry — [Microsoft even announced that it would be disabling SMBv1 in the fall](#) — the truth is a similar attack tactic has been gaining steam for quite some time: infecting targets via Remote Desktop Protocol (RDP).

RDP is a protocol developed by Microsoft as a remote management tool. It's commonly

exposed in internal networks for use in administration and support, but when it's exposed to the wider Internet it can be a beacon for attackers.

Attacks attempting to break in via SMB and RDP work in similar ways. First, attackers can simply scan the Internet for systems with open ports (port 445 for SMB; port 3389 for RDP). Tools like masscan, which can purportedly scan the entire Internet in under six minutes, make that easy. Once an open port exposing RDP is found, attackers typically attempt to brute force their way past weak or default passwords to gain execution.

In April 2017, attackers used a RDP brute force attack to infect Erie County Medical Center, a major hospital in Buffalo, New York, with the ransomware variant SamSam. More than three months later, the hospital estimated [the cost of recovery had reached \\$10 million](#).

The groups behind SamSam, CrySiS, Shade, Apocalypse, BTCWare, and other ransomware are all using RDP as an attack vector. From Q4 2016 to January 2017, [RDP attacks spreading CrySiS alone doubled](#).

RDP is a relatively easy attack vector for most organizations to secure by placing machines with RDP enabled behind a firewall and by applying strong passwords and basic access control lists (ACLs). But until more do (according to Rapid7, [more than 4 million endpoints have port 3389 open with RDP exposed](#)), criminals are going to continue to actively abuse it.

In Q2 2017, one RDP brute force attack cost a Buffalo, NY hospital \$10,000,000.

— The Buffalo News

TREND #2:

Living off the land



What we're seeing

Increasing cases of attackers abusing legitimate tools already present on the system rather than dropping malicious files on disk.

Why it's happening

Leveraging system tools and avoiding the use of malware executables is making these attacks extremely difficult for traditional security to detect.

Examples

Attacks utilizing macros, PowerShell scripts, and tools like PsExec and WMIC.

What's next

Expect use of living off the land and fileless attack techniques to continue to grow from being exceptions to being the norm.

What to do now

Disable tools and commands you don't actively need, and make sure your endpoint security doesn't just rely on file scanning or whitelisting, which these attacks can bypass.

Deeper dive

To gain access and persistence, attackers are increasingly using an organization's own system tools and processes against it.

When [the NotPetya outbreak](#) swept across the globe in June 2017, the majority of early media coverage focused on the fact that it shared similarities with the WannaCry outbreak that had infected hundreds of thousands of machines just one month before. Specifically, reports highlighted its use of the EternalBlue exploit to spread.

But NotPetya stood out from WannaCry in a number of important ways. First of all, [it was determined to be a wiper designed for destruction](#) rather than true ransomware designed for extortion. But another key reason why it was so dangerous is that it abused otherwise legitimate system tools and processes to infect its victims and spread like wildfire through compromised networks.

Victims were initially infected by installing an update for Ukrainian accounting software MEDoc. The attack then spread using PsExec and WMIC — two tools commonly associated with system administration that are already present on practically any Windows machine.

These were conscious choices on the attackers' part. To avoid raising red flags, they designed the attack to leverage otherwise legitimate tools and processes. It's an approach security experts refer to as "living off the land."

"A good hacker avoids the use of malware and code exploits whenever possible... There's no sense in using malicious code when simpler and quieter means are available."

— Lesley Carhart

As security researcher Lesley Carhart explained [in a response to NotPetya](#), "The use of [WMIC and PsExec to move laterally across a network] is not likely to fire any built-in attack signature in traditional, signature-based security tools. There's nothing to sandbox nor an unusual unique file hash to scan for. On the surface, this activity will look like administration, and might only be detected by more detailed behavioral analysis."

While "living off the land" isn't a new concept for attackers, techniques that embrace it are becomingly increasingly commonplace.

Part of the reason is the obvious benefit of hiding attacks in plain sight. By utilizing admin tools, system commands, and VB or PowerShell scripts, attackers can avoid detection while achieving execution, persistence, and lateral movement. Easy-to-use penetration testing tools like Metasploit, Powersploit, and Mimikatz — described as “[the Swiss Army knife of Windows credentials](#)” — have also played an inadvertent part in sparking widespread, downstream adoption of these techniques, making them easier to package and commoditize for criminals even if they have relatively little technical expertise.

Over 40% of organizations have experienced attacks exploiting legitimate scripting tools.

— SANS

The danger with many of these attacks is they can be conducted filelessly, without a malicious binary ever being dropped on the disk. That makes detection with security products that rely on file scanning — even ones with machine learning capabilities — impossible. And because these attacks may utilize otherwise valid system tools, application whitelisting often isn’t an effective deterrent, either.

ATTACKER GOALS	LEGITIMATE SYSTEM TOOLS
Initial infection	Macros, PowerShell, VBScript, RDP
Credential harvesting	Mimikatz, Windows Credentials Editor (WCE), pwdump
Lateral movement	PsExec, Windows Management Instrumentation (WMI), RDP
Persistence	WMI, Group Policy Objects (GPOs), Scheduled Tasks

Protecting your organization against these tactics requires implementing basic security fundamentals such as network segmentation, disabling tools you don’t need, and limiting user privileges, and it also requires utilizing security solutions that are designed to [block malicious system behaviors](#), not just malicious files based on their attributes.

TREND #3:

Worm capabilities



What we're seeing

More attacks with built-in worm components designed to make infections self-spreading and more difficult to remove.

Why it's happening

The success of WannaCry and NotPetya is inspiring attackers to revisit worms to propagate their infections more rapidly.

Examples

WannaCry and NotPetya; Emotet, QakBot, and TrickBot banking trojans.

What's next

Watch for worm modules to become commoditized, purchasable add-ons for a variety of malware.

What to do now

Prioritize security that can block these attacks during runtime, before infections have the chance to spread and get entrenched.

Deeper Dive

We're seeing more and more attacks taking a self-spreading, land-and-expand approach so they can infect as many machines in as little time as possible.

While more attention was devoted to WannaCry's use of EternalBlue, it was arguably the worm component of the attack that truly set it apart. Not only did it allow the infection to spread to other hosts in the original victim's network, it also enabled the ransomware to infect new external victims, as well, ultimately spreading to an estimated 400,000 computers in more than 150 countries.

By contrast, weeks following the WannaCry outbreak, another ransomware variant called Uiwix was spotted utilizing EternalBlue to infect victims, but without the worm component [it quickly fizzled out](#).

Thanks to its worm component, WannaCry infected an estimated 400,000 computers in more than 150 countries.

— MalwareTech

While worms have wreaked havoc before (see [Conficker](#)), the WannaCry outbreak was one of the first instances of a ransomware attack incorporating worm functionality. Thanks to its success, it was certain not to be the last.

Following WannaCry, attackers have been spotted incorporating worm and lateral movement capabilities into a variety of ransomware and other malware campaigns. NotPetya is the most high-profile to date, but other examples include [Sorebrex ransomware](#) and the [Emotet](#), [QakBot](#), and [TrickBot](#) banking trojans.

The majority of these attacks will attempt to spread by harvesting or cracking credentials, then using tools like PsExec and wmic to execute their payloads remotely. Many also attempt to propagate

by enumerating network shares, dropping copies of itself on them, and creating a service to execute them.

Because brute-force attempts are often involved, another consequence of these attacks can be triggering extremely disruptive mass account lockouts, as was the case when QakBot caused [a wave of Active Directory lockouts in May 2017](#).

Now that there's a proven blueprint for infecting large numbers of victims with this type of attack, organizations have to assume more will be coming down the pike.

Unfortunately, removing malware with worm capabilities and various persistence mechanisms after-the-fact is notoriously difficult. That makes blocking it at the very outset of an attack crucial for avoiding mass disruption to business operations as well as the hijacking of business bank accounts and data.

Companies should prioritize security that can [block these attacks during runtime](#), before infections have the chance to spread and get entrenched.

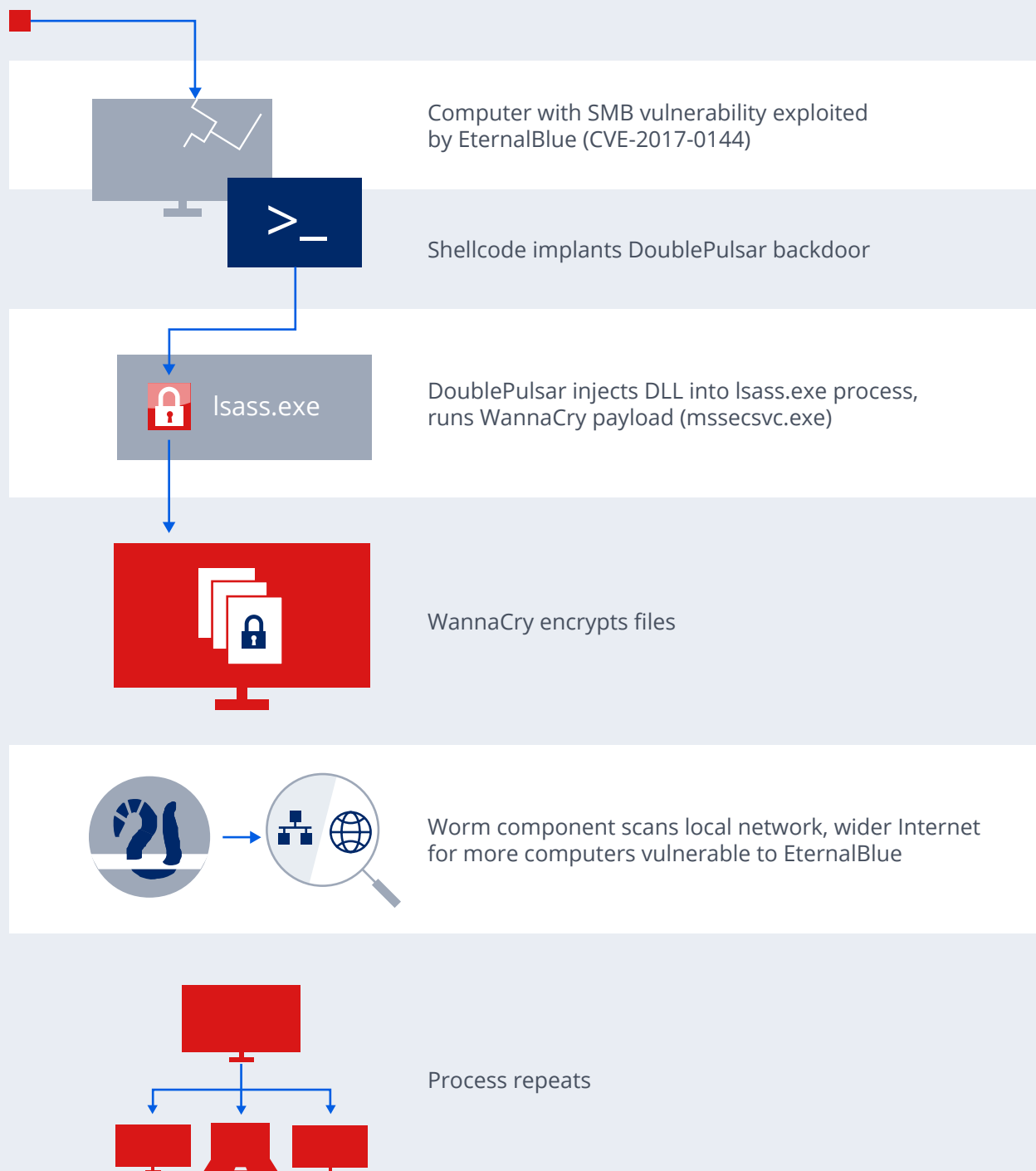
Nearly half of ransomware attacks now infect at least 20 employees in an organization.

— Intermedia

EXAMPLE ATTACK #1:

TRENDS DISPLAYED

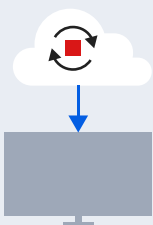
WannaCry



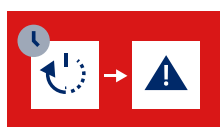
EXAMPLE ATTACK #2:

NotPetya

TRENDS DISPLAYED



Initial infection delivered via compromised software update



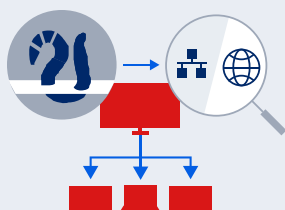
Master Boot Record (MBR) overwritten or modified to schedule a reboot and display fake error and ransom notes

SPREADING OPTION A

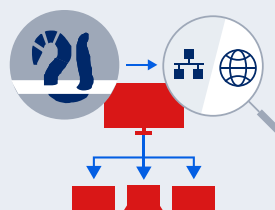


Local files encrypted with no way to recover them, even with payment

SPREADING OPTION B

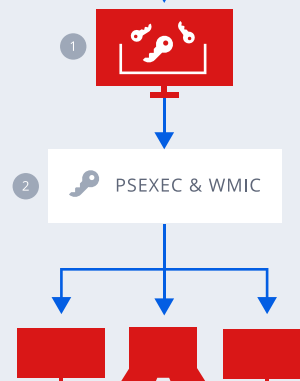


Worm component scans local network, wider Internet for more computers vulnerable to EternalBlue (CVE-2017-0144)



Worm component scans local network, wider Internet for more computers vulnerable to EternalRomance (CVE-2017-0145)

SPREADING OPTION C

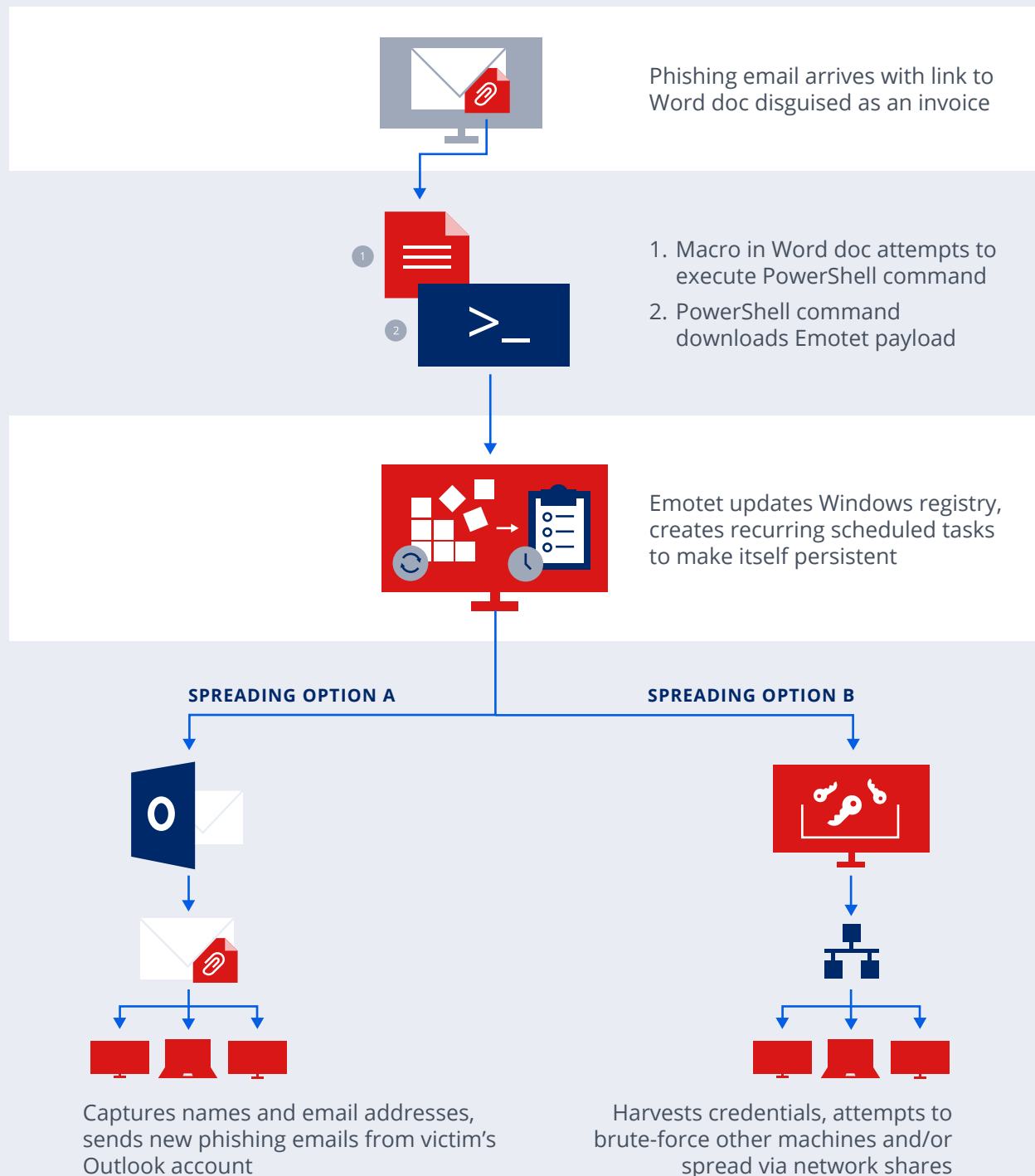


1. Credentials harvested with recompiled version of LSADump (Mimikatz)
2. Uses harvested credentials to spread through local network via PsExec and wmic

EXAMPLE ATTACK #3:

TRENDS DISPLAYED

Emotet



Protecting your organization

These latest trends in malware aren't just raising the stakes, they're also placing new demands on security. To protect themselves heading into 2018, companies need to make sure they can:

- **Prevent clickless infection**
When attacks skirt traditional infection vectors like email and compromised websites protection needs to be focused on company endpoints.
- **Respond to attacks attempting to live off the land**
When attacks use legitimate system tools rather than malicious files protection can't be limited to file scanning and whitelisting.
- **Preemptively block worm components:**
When all it takes is one infected computer to compromise an entire network it's vital to block any attacks that land on an endpoint at the very outset.

Find out how Barkly helps companies meet all three of these demands by blocking exploits, fileless, and file-based attacks before they cause any damage.

[Request a demo](#)

About Barkly

Barkly's Endpoint Protection Platform™ uses Responsive Machine Learning™ to uniquely block exploit-driven, fileless, and file-based attacks. Barkly delivers fast, lightweight protection, administered through an easy-to-use cloud service.

Learn more at barkly.com.

