Ransomware: Why 'WannaCry' Is Only the Tip of the Iceberg

Virus detection and prevention is more crucial than ever.

By Trevor Pott

The phrase "ransomware" was known by relatively few until this past May. But that all changed when a new, spectacularly successful strain of it hit the world. Its prominence garnered massive media attention, and its dangers were spelled out clearly, in ways that no white paper theorizing about potential damage could do. This damage was real, and severe. Now many people know exactly what ransomware is, and in the minds of most, it's become synonymous with "WannaCry."

WannaCry, in fact, serves as a perfect case study of the growing threat of ransomware, because it's typical of how ransomware is created and how it exploits systems and companies.

WannaCry Basics

The most important thing to understand about the WannaCry ransomware is that little about it is novel. WannaCry is not some technological terror lovingly crafted by a mad genius. Instead, it is an assemblage of parts, each of which are reasonably mundane, simple and well tested.

The WannaCry ransomware incorporates numerous elements to assist its spread. The fact that it is largely built of previously tested components has allowed its authors to regularly adapt the ransomware to overcome efforts to eliminate it. This sort of cat-and-mouse game is a normal and everyday part of the IT security world.

For ransomware to work, three basic elements are required. First, there must be a mechanism of initial infection. Second, there must be an encryption mechanism that prevents users from accessing their files. Last, there must be a demand for payment along with a means of making payment. Traditionally, ransomware authors will decrypt files if payment is made; however, in recent months there have been increasing strains of ransomware where payment does not result in decryption of files.

WannaCry adds a fourth element to the traditional ransomware cocktail: It uses a Windows vulnerability to spread beyond the initial infected computer. The result of this is that on improperly designed and improperly secured networks, one infected computer can in turn infect many others.

INSPIRING/SHUTTERSTOCK

WannaCry Detection and Prevention

WannaCry's mechanism of initial infection relies on what's known as phishing. In essence, these are scam e-mails that either contain a file that can infect your computer or entice you to click on links in the e-mail to take you to a Web site that will infect your computer. The most common versions of WannaCry are reported to use an encrypted file contained in a phishing e-mail.

Some media reports claim that the use of encrypted files makes WannaCry undetectable. This is false. Encrypted files of this nature are detectable, even with freely available e-mail filtering applications such as the E-mail Filter Appliance, or eFa (**bit.ly/2vz6hXC**), which is a community-based project.

These sorts of e-mail filters can be set to block all mail with encrypted files, block mail only from likely spam sources, or only allow encrypted mail from known trusted sources. These scanners can also be configured to allow end users to access the encrypted files, but only after reading a warning about the potential dangers. They can also be configured to send this type of mail to a systems administrator for assessment before release.

While open source solutions like eFa are somewhat cumbersome to deploy and use, commercially supported e-mail filters exist that are far more friendly. Many of today's e-mail filtering solutions are perfectly capable of blocking even unknown threats.

That WannaCry ransomware even made it into user mailboxes to be opened means that e-mail administrators made a choice to allow these types of files through without adequate protections. Alternately, e-mail administrators were inadequately resourced and relying on e-mail filtering technologies that are years—or even decades—old.

WannaCry Mitigation

Modern IT security procedures and solutions, including network microsegmentation, core resource isolation and automated incident response, could each have been used to prevent the spread of infection. Had networks been properly designed, resourced and secured, any systems that did manage to become infected would only have been able to infect a limited number of others.

The technologies needed to prevent, detect and contain these outbreaks are new, but they're no longer the bleeding edge, and well within the capabilities of health care government and enterprise IT departments.

Media reports typically focus on the patching of OSes and applications. Blame is laid on patching regimens because WannaCry used a previously patched Windows vulnerability to spread once established on a network. This is placing the blame where it doesn't belong.

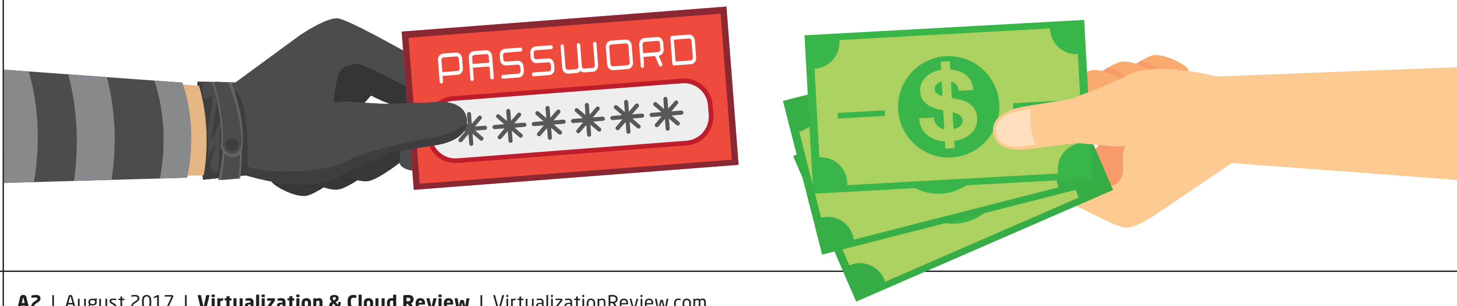
Even if an organization were to be keep all computers fully patched, this would not make those computers secure. While patching is important, perpetuating the idea that it will somehow save us is dangerous. There are dozens, if not hundreds, of unpatched vulnerabilities in the Windows OS alone. That doesn't include the various applications that run on top of Windows.

Governments and hackers alike hoard these "zero-day" vulnerabilities for use in espionage and cyber warfare. Zero-day vulnerabilities are considered precious, expensive knowledge and are used sparingly, but every now and again they find their way into some bit of malware and infect everyday systems.

Proper IT security no longer relies solely on patching computers in order to keep networks safe. "Eggshell security," in which a network has a relatively well-defended perimeter but is undefended inside that barrier, hasn't been considered adequate for more than a decade.

Systems administrators have been encouraged for years to consider every single computer on a network as unpatched and vulnerable, and design their network accordingly. WannaCry isn't the first piece of ransomware to spread from one initial point of infection across a network, and it won't be the last.

While patching is important, perpetuating the idea that it will somehow save us is dangerous.



SOLAR22/SHUTTERSTOCK

GOLDEN SIKORKA/SHUTTERSTOCK

> WannaCry is not the first piece of ransomware to spread from one initial point of infection across a network, and it won't be the last.

Patching Things Up

Some media outlets have reported that large-scale patching against WannaCry isn't possible. This is false. Patching computers in an automated fashion is not only possible, it's considered one of the most basic activities a systems administrator engages in. Windows computers can have their patches managed with Windows Server Update Services, a free feature in modern Windows Server OSes. Paid options made available by Microsoft include System Center Configuration Manager for larger deployments and Intune for smaller deployments.

Patch management isn't limited to Windows. Linux has numerous patch management options, with Red Hat's Satellite being the most popular. For those with mixed environments, an entire industry called "endpoint management" has emerged around patching and securing computers. There are hundreds of vendors selling products to patch and manage Windows, Linux and smartphones.

Patching, however, isn't straightforward. There's a lot of oversimplification occurring in media reporting regarding the WannaCry ransomware attack. Systems administrators who hadn't yet patched their systems hadn't necessarily ignored patches or warnings from Microsoft. Nor were they necessarily running unsupported software, even where Windows XP was still in use.

Patches themselves can—and sometimes do—cause computers to malfunction. A computer may work fine for years, but when a patch is applied some critical component of either the OS or an application ceases to function. Microsoft has had a number of these over the years, with several in the past several months affecting large enough numbers of people to gain media attention.

Systems administrators, especially those guarding life-critical IT, must test patches before deployment to ensure that patches don't break anything. Unfortunately, Microsoft has jettisoned its traditional Security Bulletins, and has made it increasingly difficult to learn what patches are supposed to do.

Microsoft's change to "cumulative updates" has also changed patching. Before cumulative updates, a single bad patch could be isolated and removed while all other patches were allowed to go through. With cumulative updates, systems administrators no longer have this option: You apply all patches, or none. Avoiding a damaging patch can mean being out-of-date for months or even years while waiting for Microsoft to release a patch for the broken patch. This leaves systems administrators with the choice of running potentially vulnerable, unpatched systems or trying to work around the issue.Workarounds can involve business process changes or even abandoning existing software due to incompatibility. Either option can be expensive or lead to increased errors because business processes that were automated now have to rely increasingly on human inputs.

No Easy Answers

WannaCry is just the next natural evolution in a long line of ransomware precursors. It was successful through a combination of inadequate resourcing of IT departments, the inability or unwillingness of IT departments to change, and vendors using patching as a stick.

Human nature caused WannaCry. Greed, short-sightedness and simply not cleaning up after ourselves all played their part. It will happen again, and keep happening for the foreseeable future: As a general rule, it's easier to claim, "It will not/cannot happen to me," than to learn from the mistakes of others.

Cloud computing will not save us from the WannaCries of the future. Cumulative updates aren't a social engineer panacea for our cyber ills. There are no magic bullets and no easy answers. Industry, government and individuals must work together and the question, as always, will boil down to: Who pays for it?

We, collectively, just got owned by a street thug with a shiv. It's no wonder that media outlets and experts alike rush to inflate WannaCry into something more grandiose and superlative than it really is. But those of us who work in the IT industry must remain grounded. Cyber nukes *do* exist, and like it or not, our job is to prepare for the day when they'll be used. **VCR**

Trevor Pott is a full-time nerd from Edmonton, Alberta, Canada. He splits his time between systems administration, technology writing and consulting. As a consultant, he helps Silicon Valley startups better understand systems administrators and how to sell to them.

Ransomware is a growth industry you want no part of ...

Keep your data safe and your business growing with the StorageCraft Recovery Solution

Ransomware is growing to be a billion-dollar industry, but you can protect your business's growth with frequent backups that are checked regularly and replicated to an offsite location that malware can't touch. That's just what the StorageCraft® Recovery Solution does.

StorageCraft. ShadowProtect® SPX

Automate the backing up of physical and virtual systems, applications, and data. Recover files, folders, or a whole system incredibly fast.

StorageCraft. Cloud Services™

Replicate SPX backups to the StorageCraft Cloud where they're safe from ransomware. Recover files and folders, or spin up your entire infrastructure with one click using patented technology.

Use SPX FREE for 30 Days!

www.StorageCraft.com/VIRMRAN

StorageCraft.