Ransomware:
The trap within the trap

The big distinction between ransomware and malware is that you know when the ransomware criminal comes calling. You either pay up or you lose your data. Very few of us know when an attacker owns our computer with malware, and that's the real problem, writes **Todd Rosenblum**

Ransomware is like the door closing once you've stepped on a trap. It's the backend of a sophisticated or unsophisticated attack of an individual computer, or a network of thousands of computers linked together by a central hub.

Identifying all cyber intrusions in networks, all system vulnerabilities, and getting all humans to not fall for malicious clicks is not possible. However, all of us could do much more to reduce the size of the open hole, and make it easier for cyber defenders to focus on high-end challenges. Ransomware is not going away, and attack vectors like botnet (automated)-based spear phishing attack probes, appearing as important messages or notes from friends, family and colleagues asking us to click on a hostile link, are not going away either.

The apparent North Korean ransomware attack, code named 'WannaCry' has long and deep origins, involving industry, governments, state and semi-state hackers, and the broad community of internet users. Let's break this down.

Microsoft released its widely anticipated Windows XP operating system in 2001. Like all software releases, it had flaws and errors in its basic code. Microsoft invested considerable time and energy closing, or patching, those holes upon identification. But some holes remained. Microsoft has released several newer operating systems, such as its latest offering Windows 10, and announced several years back that it was no longer offering updates to patch holes in XP. This is standard industry practice.

Since the beginning of the modern internet, criminals and governments have pursued these holes for private or public gain. Criminals use these holes to make money off, for example, stolen credit card numbers, and governments use these holes for espionage.

The US National Security Agency (NSA), widely believed to be a global leader in the digital domain, built a hacking tool into Windows XP named Eternal Blue. NSA officials exploited this hole for more than five years, and, according to unnamed NSA officials quoted in *The Washington Post*, said it led to an: "Unreal haul" of intelligence for the US Government. It was like: "Fishing with dynamite," said a second NSA official.

Eternal Blue might have been a vital tool for the NSA, but it was compromised and released by a murky Russian hacking group called the Shadow Brokers. It is not clear how the group acquired the tool, although many believe it was provided by an NSA insider. Shadow Brokers told the world about the hole in Windows XP.

Now comes North Korea. A group linked to North Korea called Lazarus has a history tied to internet-based financial crime. The Lazarus group has been active since 2009, and is deemed to be tied to the 2014 hack of Sony Pictures, the penetration last year of two Polish banks, and theft of $81 million from a bank in Bangladesh. The cyber security firm Symantec concluded there were: "Substantial commonalities," between the Lazarus group and the WannaCry ransomware attack. It appears the North Korean state is in the cyber financial crimes business.

Murky hacking

Meanwhile, the NSA, five years after it began its huge intelligence gathering haul via the hole in Windows XP, told Microsoft about the exploit once it confirmed Eternal Blue had been stolen. NSA shared its knowledge with a presumably very unhappy Microsoft before the Shadow Brokers told the world of Eternal Blue. Microsoft immediately built a patch and pushed it to registered Windows XP users, even though it had earlier said it was no longer issuing patches for this old operating system. The Department of Homeland Security concurrently informed its network of public and private sector computer users that they should immediately disable Windows XP.

The WannaCry attack was a big deal, but was not particularly successful in financial terms. Cyber expert Doug Shepherd described it as: "A poorly organised attack with a poorly constructed tool." The attack infected more than 300,000 computers and networks in more than 100 countries. The attackers demanded $300 dollars in the electronic currency Bitcoin if the victims wanted their information back, but the conspiracy yielded only $75,000 in payments.

But why were so many computers and networks compromised? Hadn't Microsoft issued a patch to close the exploit months before the WannaCry attack? Hadn't the DHS told its network of public and private users in the US about the vulnerability?

Now we get to the real vulnerability: human error.

Microsoft can issue a patch, but it can't make users install that patch. Microsoft would love its client base to upgrade from its 16-year-old operating system, but many have not. Microsoft would love its intellectual property to be protected, all its users to register their product and turn on automatic updates, and take down countless pirated versions of Windows XP still in use, especially in China.

But even at the enterprise level, updates take time to perform. Companies must co-ordinate times to limit disruption to operations, and often will test the update before issuing them to their pool of employees.

Some will blame the NSA for holding onto the vulnerability for so many years. Others assert that there must be balance in the need to gather critical national security intelligence and the need to share holes with industry.

And the problem of real human users taking the click bait is getting worse. IBM's security research unit collects and monitors 45 million pieces of spam a day worldwide. In 2015, less than one per cent of the spam was ransomware. In 2016, 40 per cent of spam contained a document or web link that activated ransomware. Even the act of spear phishing is becoming more automated. Increasingly, hackers are employing botnets to troll more, faster and longer than ever before, and attackers are now moving into fake social media requests. They are moving to Twitter feeds and fake messages from ostensible friends on Facebook. The Internet of Things is ushering in a vast new world of vulnerability.

The online world is not getting more secure, but simple steps like immediately installing updates, phasing out old, dated operating systems that are no longer supported, using real passwords, and not using pirated software, are low hanging fruit that must be taken seriously and done with great haste.

Governments and technology companies would do well to partner in promoting basic cyber hygiene. We want our cyber sleuths to focus on high-end network threat detection and mitigation, not be reminding staff to install updates. There also is promise in software to check the integrity of software. The fewer the exploits, the smaller the playing field of concerns.

Our profoundly insecure internet is here to stay, and human nature will continue to mean we will assume seemingly customised messages, tweets and friend requests are what they say they are. We will mitigate and manage the threat, not eliminate it. Perhaps more states will stop giving refuge to hackers and the cost of doing illegal business will go up greatly. Maybe there will even be a day when all states realise that fostering semi-state hackers will come back to bite them.

After all, the largest concentration of WannaCry victims were in China and Russia. CRJ

At a glance

WannaCry ransomware attack was a: "A poorly organised attack with a poorly constructed tool," and although immensely disruptive, not particularly successful in financial terms

The key is reducing the human vulnerability factor, allowing cyber defenders to focus on high-end challenges

The ransomware threat can only be managed and mitigated, not eliminated

States providing refuge to hackers should rethink; those fostering semi-state hackers should realise this could come back to bite them

Author

TODD M ROSENBLUM *is a former senior Defense and Homeland security official in the United States government, a Fellow at The Atlantic Council, and a Senior Executive for National Security at IBM*