What We Learned From the WannaCry Ransomware Attack

By Greg Patterson

It is likely that you have heard of the WannaCry ransomware attack, one of the most widespread cyber-attacks to date. Security experts estimate that more than 200,000 users have been infected with this malware. Once infected, all information on the user's computer is encrypted (i.e., locked away) unless a ransom of $300 to $600 is paid to the attackers in Bitcoin. To make matters worse, there is no evidence that the attackers have ever held up their end of the deal. Generally, when a user pays, the encrypted information is *not* returned in its normal state. In other words, this global attack just leaves the information irrecoverable.

You might be wondering what you could possibly do to defend against WannaCry and similar attacks in the future. Let's review four valuable lessons that this recent event has taught us about protecting ourselves.

Lesson #1: Keep up with security news to raise awareness of current threats. Over Easter weekend, a notorious hacker group called the Shadow Brokers leaked confidential National Security Agency (NSA) hacking tools and techniques, including a number of critical Microsoft vulnerabilities. Just a few weeks later, WannaCry struck, taking advantage of one of those vulnerabilities. If we had all read the news about the NSA leak, we would have been warned that our Microsoft software was wide open to an attack. But even if we had been able to follow these breadcrumbs, what could we have done? That's where Lesson #2 comes in.

Lesson #2: Don't delay your updates. When news of the NSA leak first broke in April, Microsoft immediately stated that it had released an appropriate security patch. In fact, it had released the patch in March—*one month before* the NSA leak. Sounds as if we should have been all set, right? That would have been true had we all updated our machines on time. Unfortunately, when we are at our computers and an update box appears, we sometimes delay installation because we do not want to be interrupted. But system updates often include critical security patches that protect us from current cyber-attacks. Delaying their installation only leaves us vulnerable for a longer period of time.

It turns out that *all* 200,000 victims of the WannaCry ransomware attack had unpatched systems. Though the attack struck in May, these users had not updated their Windows operating systems (and subsequently rebooted their computers) since before March, so the patch had not taken effect.

The next time you are prompted for an update, keep in mind that it might be the one thing that could protect you from attacks like WannaCry. If you have to delay installation, do not delay for too long.

Lesson #3: If you need that information, back it up. The single most important safeguard against ransomware is backups. If you back up all your important information—and your machine becomes infected with ransomware—you already have a duplicate of everything the attackers are holding for ransom, and there is no need to even consider paying. But backups are only effective if done right. When adopting a backup process, keep these three tips in mind:

- Your backup should be stored separately from the system you're backing up. If you perform local backups on an external hard drive, leave it unplugged from your system when it isn't backing up. If you have a cloud provider, research the protections it has in place to defend against ransomware infections. (Cloud providers typically offer versioning, which allows you to roll back to an uninfected version of your files if the files are ever infected or corrupted.)
- Regularly test your backups. Imagine believing that you are protected against ransomware only to be attacked and find that you can't restore your backup properly. It is worth ensuring that the process works. Test a restore from time to time.
- Secure your backup information as much as you would your original information. When backing up sensitive information, be sure that it is encrypted and password protected. If it is a physical hard drive, keep it in a place where no one can easily take it.

Lesson #4: Honor among thieves isn't always a reality. Believe it or not, upon payment, a majority of ransomware attackers actually give users their information back. Unfortunately, in the case of the WannaCry variant, experts believe that the attackers *do not* give the information back—no matter what. So when confronted with WannaCry, we recommend doing as the evidence suggests—do not pay.

If you are hit with any other variant of ransomware, we cannot tell you what to do. If you search for answers online, you will see that some experts recommend never paying. But, ultimately, that decision is up to you. Always research the particular variant for possible alternative solutions, and keep in mind that no one but you can safely say what your information is worth.

Preventing disaster before it's too late. Many of us do not take action until we are part of a major database breach. Yet we should always be preparing for such threats. As we have seen with WannaCry, there were ways its victims could have prevented being affected. There is no telling what major cyber-attack will be in the news next. But if we take the time to find the lessons in the last attack—and apply them to our own lives—we will be in a much better position to defend our information when the worst happens.

This Month's Puzzle Solutions

P	A	T	S	■	D	I	S	C	S	■	D	O	G	S
U	T	A	H	■	E	B	O	L	A	■	U	N	I	T
M	O	R	E	■	L	I	B	E	R	A	L	I	Z	E
A	P	P	L	A	U	D	■	W	I	N	S	O	M	E
■	■	■	L	X	X	■	■	■	■	T	E	N	O	R
D	E	F	I	L	E	M	E	N	T	S	■	■	■	■
U	R	I	N	E	■	E	M	E	R	Y	■	H	I	P
P	A	N	G	■	D	E	C	A	Y	■	W	A	D	I
E	S	E	■	M	E	T	E	R	■	T	A	R	O	T
■	■	■	■	O	B	S	E	S	S	I	V	E	L	Y
O	C	T	A	L	■	■	■	■	I	R	E	■	■	■
U	L	U	L	A	T	E	■	S	N	O	O	K	E	R
T	O	L	E	R	A	T	I	O	N	■	F	A	D	O
E	V	E	R	■	M	U	R	R	E	■	F	L	I	T
R	E	S	T	■	P	I	K	E	R	■	S	E	T	S

1	5	9	7	8	3	6	4	2
6	8	4	9	5	2	7	3	1
7	2	3	1	6	4	5	9	8
3	7	1	4	2	5	8	6	9
4	9	2	6	7	8	1	5	3
5	6	8	3	9	1	2	7	4
9	1	5	8	3	6	4	2	7
8	3	6	2	4	7	9	1	5
2	4	7	5	1	9	3	8	6