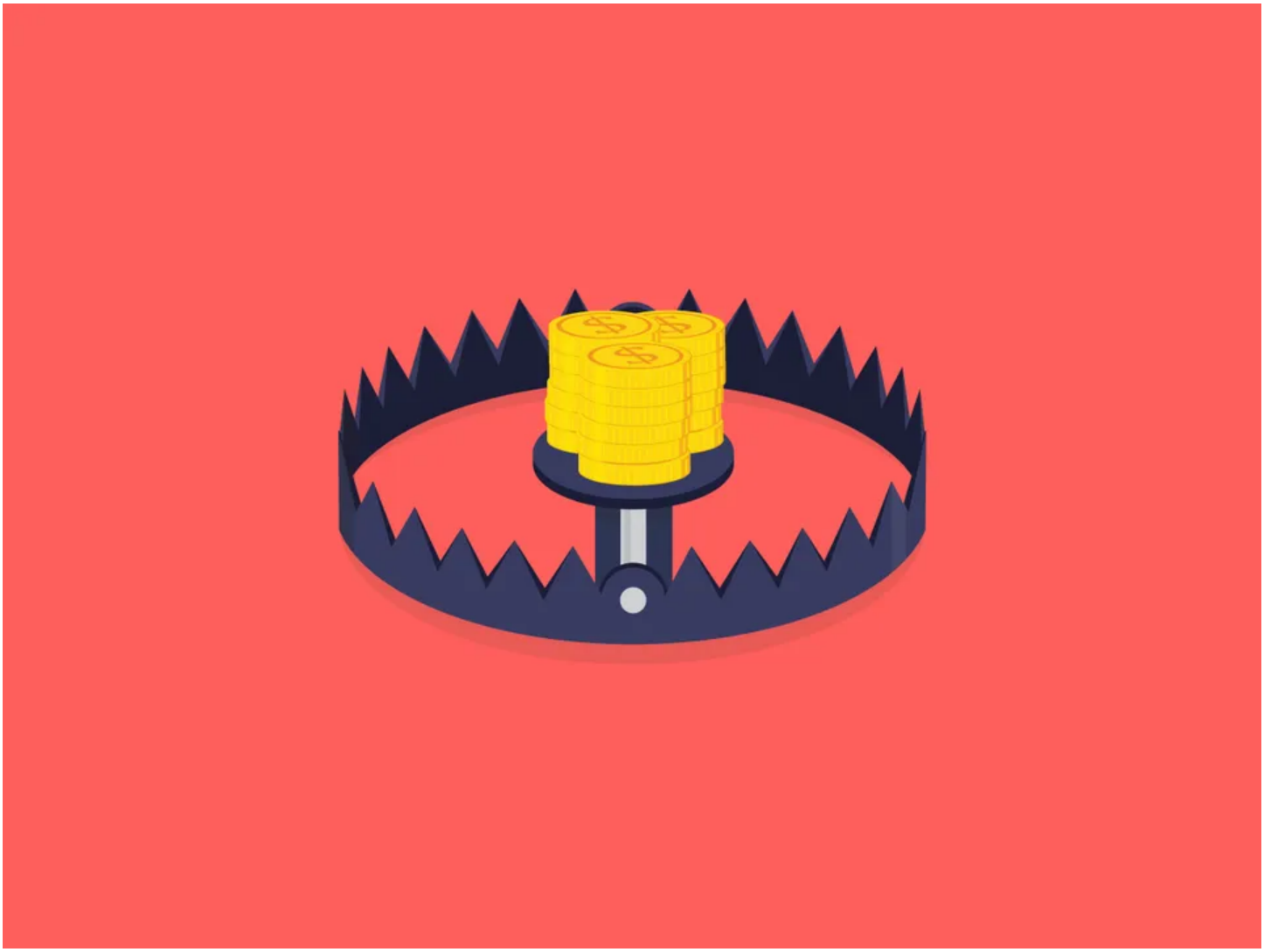
ANDY GREENBERG SECURITY MAY 15, 2017 2:43 PM

The WannaCry Ransomware Hackers Made Some Real Amateur Mistakes

Researchers say the worst ransomware epidemic ever is also poorly run, shoddily coded, and barely profitable.



GETTY IMAGES

THE WannaCry ransomware attack has quickly become the worst digital disaster to strike the internet in years, crippling transportation and hospitals globally. But it increasingly appears that this is not the work of hacker masterminds. Instead, cybersecurity investigators see in the recent meltdown a sloppy cybercriminal scheme, one that reveals amateur mistakes at practically every turn.

As the unprecedented ransomware attack known as WannaCry (or Wcrypt) unfolds, the cybersecurity community has marveled at the inexplicable errors the malware's authors have made. Despite the giant footprint of the attack, which leveraged a leaked NSA-created Windows hacking technique to infect more than 200,000 systems across 150 countries, malware analysts say poor choices on the part of WannaCry's creators have limited both its scope and profit.

More WannaCry

The Ransomware Meltdown Experts Warned About Is Here →

How an Accidental 'Kill Switch' Slowed Friday's Massive Ransomware Attack →

If You Still Use Windows XP, Prepare For the Worst →

Those errors include building in a web-based "kill-switch" that cut short its spread, unsavvy handling of bitcoin payments that makes it far easier to track the hacker group's profits, and even a shoddy ransom function in the malware itself. Some analysts say the system makes it impossible for the criminals to know who's paid the ransom and who hasn't.

An attack of this magnitude involving so many missteps raises plenty of questions while delivering a sobering reminder: If actual cybercriminal professionals improved on the group's methods, the results could be even graver.

Mistakes Were Made

At last count, the group behind WannaCry has earned just over $55,000 from its internet-shaking attack, a small fraction of the multimillion-dollar profits of more professional stealthy ransomware schemes. "From a ransom perspective, it's a catastrophic failure," says Craig Williams, a cybersecurity researcher with Cisco's Talos team. "High damage, very high publicity, very high law-enforcement visibility, and it has probably the lowest profit margin we've seen from any moderate or even small ransomware campaign."

Those meager profits may partly stem from WannaCry barely fulfilling its basic ransom functions, says Matthew Hickey, a researcher at London-based security firm Hacker House. Over the weekend, Hickey dug into WannaCry's code and found that the malware doesn't automatically verify that a particular victim has paid the demanded $300 bitcoin ransom by assigning them a unique bitcoin address. Instead, it provides only one of four hardcoded bitcoin addresses, meaning incoming payments don't have identifying details that could help automate the decryption process. Instead, the criminals themselves have had to figure out which computer to decrypt as ransoms come in, an untenable arrangement given the hundreds of thousands of infected devices. "It really is a manual process at the other end, and someone has to acknowledge and send the key," says Hickey.

Hickey warns that the setup will inevitably lead to the criminals failing to decrypt computers even after payment. He says he's already been monitoring one victim who paid more than 12 hours ago and has yet to receive a decryption key. "They're not really prepared to deal with an outbreak of this scale," Hickey says.

Using only four hardcoded bitcoin addresses in the malware not only introduces the payments problem but also makes it far easier for the security community and law enforcement to track any attempt to anonymously cash out WannaCry profits.

All bitcoin transactions are visible on bitcoin's public accounting ledger, known as the blockchain.

"It looks impressive as hell, because you think they must be genius coders in order to integrate the NSA exploit into a virus. But in fact, that's all they know how to do, and they're basket cases otherwise," says Rob Graham, a security consultant for Errata Security. "That they have hardcoded bitcoin addresses, rather than one bitcoin address per victim, shows their limited thinking."

Cisco researchers say they've found that a "check payment" button in the ransomware doesn't actually even check if any bitcoins have been sent. Instead, Williams says, it randomly provides one of four answers---three fake error messages or a fake "decryption" message. If the hackers are decrypting anyone's files, Williams believes it's through a manual process of communication with victims via the malware's "contact" button, or by arbitrarily sending decryption keys to a few users to give victims the illusion that paying the ransom does free their files. And unlike more functional and automated ransomware attacks, that janky process provides almost no incentive for anyone to actually pay up. "It breaks the entire trust model that makes ransomware work," Williams says.

Scale Over Substance

To be fair, WannaCry has spread with a speed and scale that ransomware has never achieved before. Its use of a recently leaked NSA Windows vulnerability, called EternalBlue, created the worst epidemic of malicious encryption yet seen.

But even judging WannaCry solely by its ability to spread, its creators made huge blunders. They inexplicably built a "kill switch" into their code, designed to reach out to a unique web address and disable its encryption payload if it makes a successful connection. Researchers have speculated that the feature might be a stealth measure designed to avoid detection if the code is running on a virtual test machine. But it also allowed a pseudonymous researcher who goes by the name MalwareTech to simply register that unique domain and prevent further infections from locking up victims' files.

'It has probably the lowest profit margin we've seen from any moderate or even small ransomware campaign.'

– CRAIG WILLIAMS, CISCO TALOS

Over the weekend, a new version of WannaCry appeared with a different "kill switch" address. Dubai-based security researcher Matt Suiche registered that second domain almost immediately, cutting short the spread of that adapted version of the malware, too. Suiche can't imagine why the hackers haven't yet coded their malware to reach out to a randomly generated URL, rather than a static one built into the ransomware's code. "I don't see any obvious explanation for why there's still a kill switch," Suiche says. Making the same mistake twice, especially one that effectivly shuts WannaCry down, makes little sense. "It seems like a logic bug," he says.

All of which has vastly limited WannaCry's profits, even as the ransomware has shut down life-saving equipment in hospitals and paralyzed trains, ATMs, and subway systems. To put the hackers' five-figure haul in perspective, Cisco's Williams notes that an earlier---and much less publicized---ransomware campaign known as Angler took in an estimated $60 million a year before getting shut down in 2015.

In fact, WannaCry has caused so much damage with such little profit that some security researchers have begun to suspect that it may not be a money-making scheme at all. Instead, they speculate, it might be someone trying to embarrass the NSA by wreaking havoc with its leaked hacking tools---possibly even the same Shadow Brokers hackers who stole those tools in the first place. "I absolutely believe this was sent by someone trying to cause as much destruction as possible," says Hacker House's Hickey.

Speculation aside, the hackers' sloppy methods also carry another lesson: A more professional operation could improve on WannaCry's techniques to inflict far worse damage. The combination of a network-based self-spreading worm and the profit potential of ransomware won't go away, says Cisco's Williams.

"This is obviously the next evolution of malware," he says. "It's going to attract copycats." The next set of criminals may be far more skilled at fueling the spread of their epidemic---and profiting from it.