NotPetya computer hack a warning to get serious about IT security

by: Roy Edroso

Published Jul 17, 2017
Last Reviewed Jul 12, 2017

Compliance

As a new computer hack hits health care facilities, experts advise you to tighten up security – not just in expected ways, but also in areas such as password and permission management.

In the last week of June, a foreign-born computer malware attacked the systems of several U.S. companies – including Princeton Community Hospital in Princeton, W.Va., and Heritage Valley Health System in Beaver, Pa.

This "NotPetya" malware is named after the 2016 Petya ransomware that it superficially resembles, according to Steven J. Hausman of Hausman Technology Presentations in Gaithersburg, Md. But it's not really ransomware, and despite its so-far limited reach, that's what makes it so frightening.

Ukrainian connection

Health IT people will remember the WannaCry ransomware that attacked health care facilities in the U.S. in May (*PBN 5/22/17*). Both WannaCry and NotPetya are related to the EternalBlue exploit, explains David Harlow, principal of The Harlow Group LLC health care law consultancy and proprietor of the HealthBlawg blog. EternalBlue is one of the "zero-day" (i.e., previously unknown) vulnerabilities stockpiled by the National Security Administration (NSA) and hacked and released by the hacker group Shadow Brokers. "This is a Windows vulnerability that has been patched by Microsoft in currently supported versions of Windows," says Harlow.

WannaCry was a "massive" phenomenon – "like a pandemic," says Ken Dort, a partner in Drinker Biddle's IP Group and the chairman of the firm's Technology Committee in Chicago – that indiscriminately hit about 250,000 companies, demanding relatively small payments from each.

NotPetya, on the other hand, has only hit a few companies, and its users don't ask for money – or, when they do ask, don't release the data upon payment, as is usual with ransomware, for a simple reason: The data is not held but completely destroyed. Apparently the original perpetrators maliciously targeted specific businesses in Ukraine and Eastern Europe via the software updater of a popular product in that area, M.E. Doc, and then it got out of hand. "It was not set up for ransom per se; it just destroyed the data," says Dort. "So there was no endgame of letting it out for payment."

The group behind NotPetya "either didn't fully understand the potential impact of their malware or considered the fall-out as convenient collateral damage as it spread beyond the M.E. Doc users," says Brian Chappell, senior director, enterprise & solutions architecture for BeyondTrust in the U.K. The other systems that got hit as the exploit spread across Europe into the U.S.

On the rise?

Most of the experts who spoke to *Part B News* thought the threat to businesses – including health care businesses – is increasing and sufficiently indiscriminate that no one can ignore it.

"Ransomware is on the rise," says Dort. "Like any business model, if it seems to be working you'll get a lot of copycats." "Ransomware isn't new, but the scale of the attacks is larger and the attackers themselves are getting bolder," says Michael E. Rubin, director of communications for Patientory in. "Exploits like EternalBlue will continue to be used by a wide variety of hackers from one-off individuals to nation state attacks and ransomware," says Blake J. Darché, co-founder and chief security officer of Area 1 Security in Redwood City, Calif.

Even absent a profit motive, you can expect more invasive and destructive exploits in the future. NotPetya "speaks to a growing trend in the ease of executing destructive activity on computers," Mark Defresne, director of threat research and adversary prevention for Endgame in Arlington, Va. "We do not know enough to confidently advise that threat actors motivations are changing from a means of monetary gain to business or presumed infrastructure disruption," adds Dave McKnight, a senior manager at Crowe Horwath LLP in Chicago; "however, that is the presumed trend the security industry is postulating."

6 tips to beat the hacks

- **Patch.** Everyone's supposed to but, surprisingly, many companies don't use the security patches their software vendors send them. "It is common for me to find business owners who haven't installed Windows Updates for over a year," says Julian Jacobsen, founding partner at J.J. Micro IT Consulting, O'Fallon, Mo. "Even businesses who are staying on top of updates aren't disabling the SMBv1 protocol on their servers and network."

"Most of these holes are patched immediately by the manufacturer -- Microsoft in this instance -- but any patch requires that the end-user apply them," says Al Alper, founder and CEO of Absolute Logic in Wilton, Conn. "Truth be told, Wannacry, Petya, NotPetya, etc., would have no audience had systems been properly protected."

- **Whitelist.** It's restrictive, but it "prevents the installing of any software unless it is already approved," says Steven J.J. Weisman, identity theft expert and founder of Scamicide.com. "This will keep ransomware from being installed even if an employee mistakenly clicks on a link containing ransomware."

- **Use security professionals.** Companies "may rely on IT professionals – internal or outsourced – that are not security engineers," says Alper. "They are excellent at IT but not security-related exploits, products and mitigation opportunities."

- **Isolate data.** Use a policy of "data minimization" – which McKnight describes as "making conscious choices on the location and accessibility of their data and services that store, process or transmit data, both internet facing and internally." Some experts also refer to "network segmentation," whereby some data that may have had more or less continuous exposure to outside networks will instead be shifted to limited or even no exposure to those networks.

Your backup systems should be isolated to the extent possible, as well – "air-gapped," as Harlow puts it. That should be "set up in a defensive posture — that is, backup that continually replicates and is stored separately from your live system," says Dort. "If it's connected to the live system, its value as a backup goes away. If the contamination gets into the backup, what's the point?"

- **Restrict password and privilege policies.** Chappell recommends "privileged password management" – including different, complex and unique passwords for each of the administrator accounts on every system and domain/directory administrator passwords that are changed after every use, ideally via a privileged password manager (PPM).

Under such a program, a user might request and receive access to a privileged account, do whatever work they need to do and then check the account back into the system – at which point the PPM changes the password.

Finally, "employ least-privilege tools to give users targeted, robust and safe access to elevated privileges only where needed," says Chappell.

- **Train imaginatively.** Don't just give entry-level PowerPoint training. Use more involving methods. For example, "run fake phishing attacks on a random basis," says Harlow. "If an employee clicks on a link, he or she is directed to an educational website. … Run training tailored to the organization and to the individuals receiving the training, based on their everyday responsibilities. Canned training becomes white noise ignored by staff." – *Roy Edroso (redroso@decisionhealth.com)*

BACK TO TOP

Part B News COLLECT EVERY DOLLAR YOUR PRACTICE DESERVES

PART B NEWS

- PBN Current Issue
- PBN User Tools
- PBN Benchmarks
- Ask a PBN Expert
- NPP Report Archive
- Part B News Archive

CODING REFERENCES

- ICD-9 CM Guidelines
- E&M Guidelines
- HCPCS
- CCI Policy Manual
- Fee Schedules
- Medically Unlikely Edits (MUE)
- PQRI
- Medicare Transmittals

Subscribe | Log In | FAQ | CEUs

POLICY REFERENCES

- Medicare Manual
  - 100-01
  - 100-02
  - 100-03
  - 100-04

JOIN OUR COMMUNITY!

Like us on Facebook

Follow us on Twitter

Join us on LinkedIn

Read and comment on the PBN Editors' Blog

Participate in PBN Discussion Forum

Contact the Part B News Editors

DECISIONHEALTH

Enhance your *Part B News* experience – other DecisionHealth Medicare websites:

Part B Answers RBRVS FeeCalc

Copyright © 2017 DecisionHealth. All rights reserved.
CPT © 2016 American Medical Association. All rights reserved.
Privacy Policy | Terms & Conditions