Threat of the Month: SMB and the return of worms

What is it?

SMB is a networking protocol that can facilitate computer-to-computer interactions such as file sharing, network printing, or connecting various devices. SMB was once one of the most popular protocols for sharing files over the network, thanks to Microsoft's adoption, implementation, and investment in it, beginning in the early 1990s. Setting up and using SMB within Windows was easy, requiring very little configuration, and worked for a variety of purposes. It was a seamless experience: you could access files on a remote computer as though they were on the local machine. You don't need a server to communicate between the computers—they can connect directly.

Why should you care?

The convenience provided by SMB has its dark side. Naturally, being a protocol for computer-to-computer communication, it becomes a target for attackers looking to traverse a network. It is also a natural choice for malicious actors developing worms to spread across a network, jumping from one computer to the next, leaving their malicious payloads behind as they go.

What threats target SMB?

A major exploit for SMB, called EternalBlue, was uncovered in 2017. This exploit could help attackers to install malware on a vulnerable computer. Shortly thereafter, the WannaCry threat appeared on the threat landscape, utilizing EternalBlue to spread. The Nyetya threat followed the subsequent month. While not utilizing EternalBlue, plenty of other threats have leveraged SMB to compromise computers, including SamSam, Bad Rabbit, and Olympic Destroyer.

Why does it matter?

SMB has been a convenient option for setting up computer-to-computer networking within a local network. However, that ease of use comes with its share of risk. There was little-to-no authentication when connecting to shares and the connections did not leverage encryption. While its security improved in later versions, backwards compatibility meant that older versions continued to work long after they had been found to be insecure. Given how the protocol can connect computers, it became a natural target for hackers and worms.

Further reading

https://blog.talosintelligence.com/2017/05/wannacry.html

https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html

https://blog.talosintelligence.com/2018/01/samsam-evolution-continues-netting-over.html

https://blog.talosintelligence.com/2017/10/bad-rabbit.html

https://blog.talosintelligence.com/2018/02/olympic-destroyer.html

CXX-XXXXXX-00 01/19

What Should I do?

The easiest solution is to stop using SMB, since there are few reasons to continue to use it today. Instead of sharing files by linking computers via SMB, use a dedicated file server or a cloud-based offering. Configure network printers to use other protocols. If you cannot turn off SMB in your environment, at least ensure SMB1 is disabled. Block TCP ports 445 and 139 at the network boundary to ensure SMB communication is limited to the internal network. Beyond that, endpoints should not be able to communicate with one another via SMB.

How does Cisco protect you?

Next-Generation Firewalls/Next-Generation Intrusion Prevention System	Detects and blocks malicious traffic associated with SMB attacks.
Advanced Malware Protection (AMP) for Endpoints	Continuous monitoring and retrospective security capabilities stop threats using SMB.
Cisco Stealthwatch®	Detects connections to SMB shares, correlating this activity to alert administrators.
Threat Grid	Helps identify malicious file behavior and automatically informs all Cisco Security products.