SophosLabs surveys the threat landscape for 2020 trends

SophosLabs Uncut

5 NOVEMBER 2019

By Andrew Brandt

SophosLabs this morning published its annual assessment on the state of internet and information security, and our outlook on what security threats are likely to affect the world in the coming year: the SophosLabs 2020 Threat Report, available for download now.

This year, our report broadens the scope of our analysis to cover topics beyond Sophos' historic core-competencies in desktop malware and spam prevention to more accurately reflect the broader range of security issues the company helps customers address and mitigate today.

While the report discusses bread-and-butter topics like ransomware tools and techniques, novel mobile malware, and the persistent onslaught of automated attacks on devices at the network's edge, it also covers, for example, issues surrounding securing cloud computing services and instances, and attacks targeting some of the same machine learning methods Sophos uses to enhance its detection of malicious activity.

Attacking like a boss

You might also enjoy...

11 OCT

CORPORATE • NETWORK

XG Firewall v18 early access is now available

01 OCT

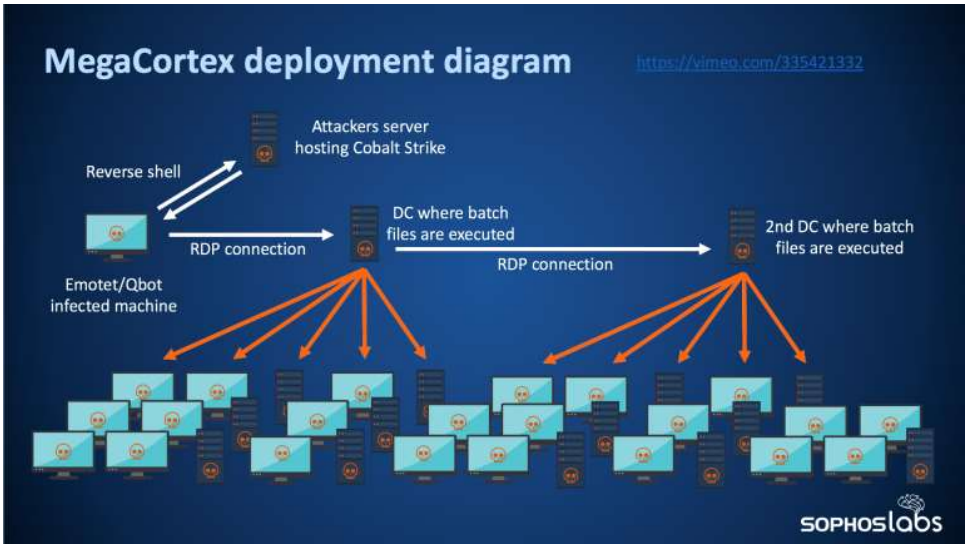
CORPORATE • SOPHOS PRODUCTS

Sophos launches Managed Threat Response service

05 MAR

We've named one of the big trends that's been on the rise in 2019 *automated active attacks*; These involve human-directed compromise of internal networks, followed by the use of standard Windows network administration tools such as WMI and PowerShell to rapidly distribute malware throughout a large enterprise network all at once.

This method was used, for example, by the threat actors behind the SamSam ransomware, and later adopted by other threat actors involved in the distribution of ransomware targeting large networks, such as the criminals behind the MegaCortex ransomware.



These complex attacks follow a predictable pattern that involve the use of open-source security tools, and compromised Domain Administrator credentials, to leverage the network's own infrastructure against itself.

Criminals run roughshod over RDP

The Remote Desktop service and its client application have been essential Microsoft network management tools for years, but 2019 saw a significant leap in both "shotgun" and targeted attacks against this standard Windows component. While some attackers chose their targets carefully, leveraging vulnerabilities in RDP and engaging in brute-force login attacks against RDP services operated by their targets, others seem to scan the entire internet looking for an open RDP machine.

The perpetual flood of scan traffic gave rise to a question: How long, we wondered, could a machine that exposed RDP to the public-facing internet remain uncompromised and unaffected by the neverending waves of attacks. To find out, we built honeypot servers, designed to look to the world like a vulnerable machine poking through a firewall, and distributed them to data centers around the world. We didn't advertise their existence or make them noticeable in any way, but the attackers found them anyway, rapidly. The results were somewhat shocking.

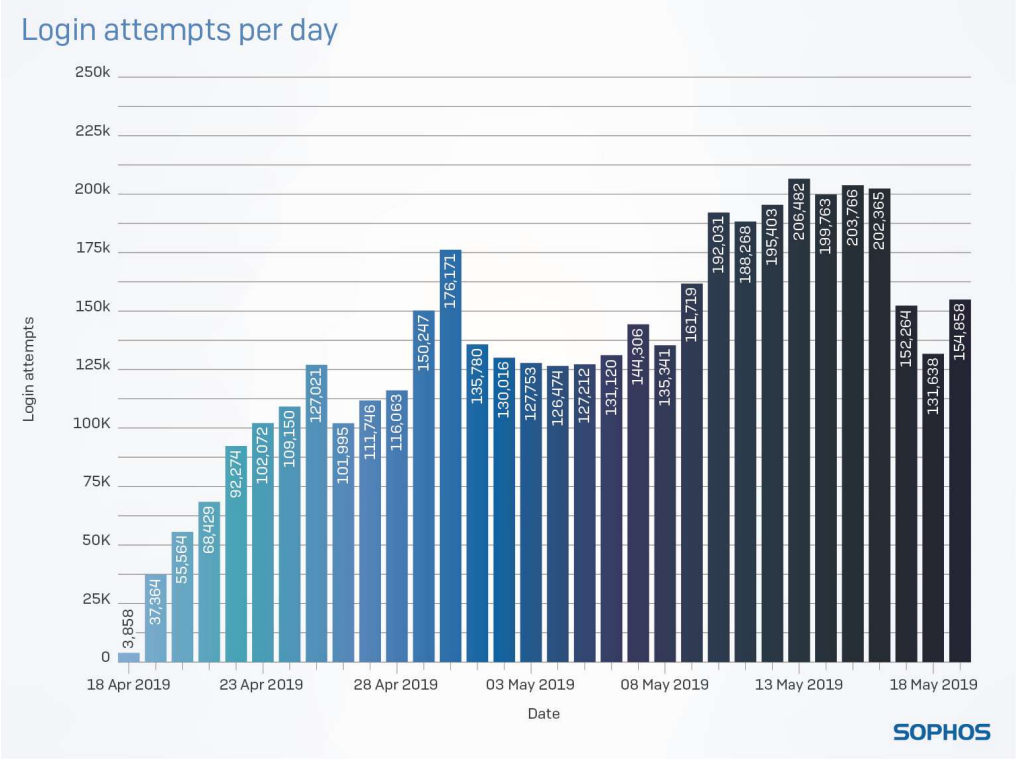
CORPORATE • SOPHOS PRODUCTS

Intercept X Achieves Highest Scores in NSS Labs 2019 Advanced Endpoint Protection (AEP) Group Test

25
JUL

CORPORATE • ENDUSER • SERVER

Sophos ranks #1 for endpoint protection by SE Labs



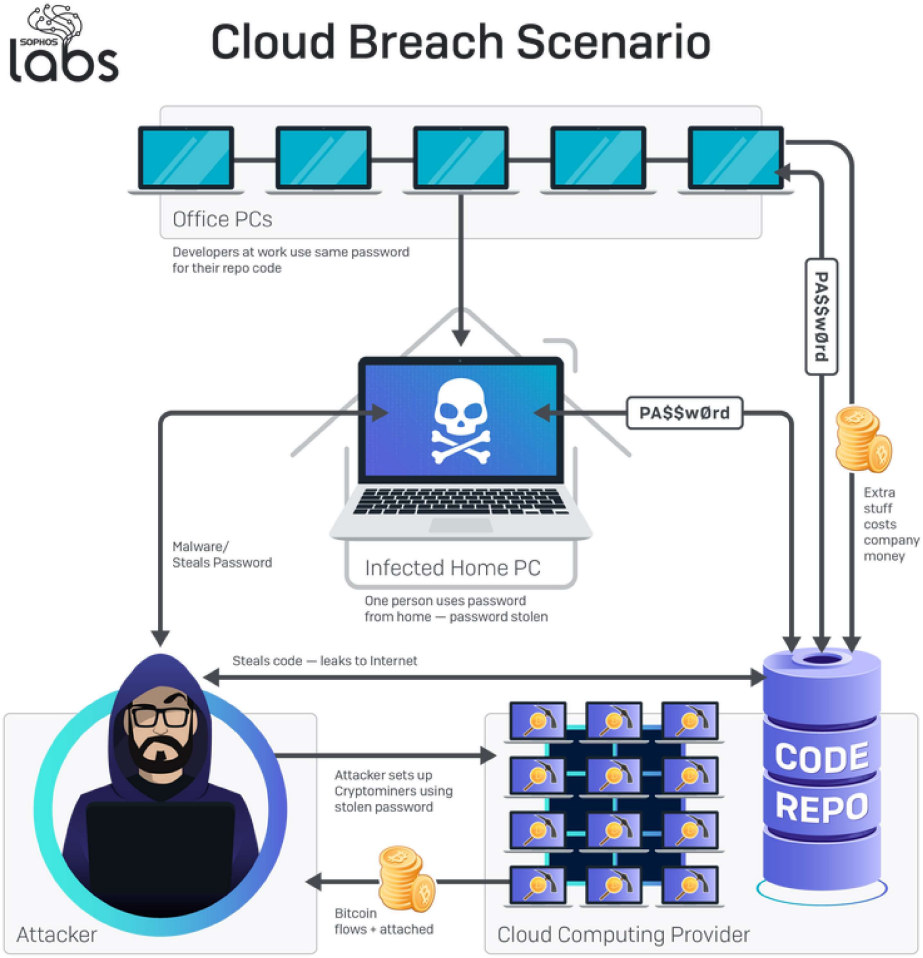
Over the course of a 30-day period this past spring, we recorded more than 3 million attempts to log in to our fake RDP servers. Note that these were not merely scans of the network port used by default by the RDP service, but active login attempts that failed only because our honeypot wasn't a real machine the potential attackers could log in to.

The lesson for network administrators is pretty clear: If you care about securing your network, make sure there isn't a single machine poking through the firewall, listening for inbound RDP connections. Because, attackers will come knocking, surprisingly fast.

Cloud security: Knowing is half the battle

Another trend we've observed is the increasing pace at which people have been, serendipitously, stumbling upon large treasure-troves of valuable, private data that have been moved (legitimately, by the data's rightful owners) into cloud computing instances and then inadequately secured from public access. Some of the cloud breaches over the past year have struck large manufacturers, financial services providers, and entertainment companies; These sting because they were avoidable.

We've pulled together a hypothetical scenario to highlight how small mistakes can create large problems. In our scenario, an organization makes a poor choice about password management, and it results in a pair of challenging problems: First, a cloud data lake becomes compromised, leading to a breach of customer information and private source code; Later the attacker who stole the password to the organization's cloud services account also uses it to set up a large number of virtual servers for the sole purposes of acting as cryptocurrency miners.



The company that lost control of its crown jewels then finds the attacker has added insult to injury by dramatically driving up the cost of the cloud computing instance, charged to the victim—all so the criminal can earn a few Monero or Bitcoin, worth far less than the costs incurred by running all those servers just to mine them.

For more on all these topics, please give our 2020 Threat Report a read.

PREV Exposed: The cost of errors in the public cloud

About the Author

Andrew Brandt

Andrew Brandt is a Principal Researcher for Sophos, specializing in security analytics and the forensic, retrospective analysis of malware infections and cyberattacks. In essence, he does whatever it takes to make life and business difficult for cybercriminals, spies, and other Internet miscreants.

Prior to joining Sophos, Brandt was the Director of Threat Research at Symantec, and at Blue Coat systems before they were acquired by Symantec. He also worked as the Lead Threat Research Analyst at

Webroot, and was an editor at PC World, covering security and privacy, for nearly a decade.

Leave a Reply

Enter your comment here...

This site uses Akismet to reduce spam. Learn how your comment data is processed.