To me myself CC / BC

symantecHW

1. What is formjacking?
   The use of malicious java script code to steal credit card details and other information from payment forms on the checkout webpages of eCommerce sites

2. How many websites are compromised each month with formjacking code?
   The average number is 4,800 per month

3. What is Powershell?
   A more powerful command line interface that combines the old command prompt with built-in scripting environment that can be leveraged to gain access to a system

4. What was the annual percentage increase in malicious Powershell scripts?
   1000%

5. What is a coinminer?
   Takes place inside web-browsers and is implemented using script languages to "mine" for Cryptocurrency

6. How much can data from a single credit card can be sold for?
   $45

7. How did Magecart successfully attack Ticketmaster?
   Magecart compromised a 3rd party chat bot, which loaded malicious code into the web browser of visitors to ticketmaster's website with the aim of harvesting customer's payment data

8. What is one reason why there has been a growth of formjacking?
   The drop in cryptocurrencies value

9. Cryptojacking dropped by what percentage between January and December 2018?
   52%

10. If a web page contains a coinmining script, what happens?
    webpages visitors computing power will be used to mine cryptocurrency for as long as the web page is open

11. How does an exploit kit work?
    Through email campaigns

12. What does the criminal group SamSam specialize in?
    Ransomware Attacks

13. How many SamSam attacks did Symantec find evidence of in 2018?
    67

14. Even though ransomware attacks declined in 2017-2018, what was one dramatic change that occurred?
    Enterprises accounted for 81% of all ransomware infections, up 12% in 2018

15. In 2018, what was the primary ransomware distribution method?
    Email Campaigns

16. What operating systems do most types of ransomware attacks still target?
    Windows based operating systems

17. What are "living off the land" attacks? What is the advantage to hackers?
    Uses generally available tools to carry out attacks that exist in the target environment that does not use malicious code

18. What is an example of a tool that's used in "living off the land" attacks?
    Worms that use simple techniques including dumping and passwords from memory or brute-forcing access to network shares to laterally move across a network

19. What are zero-day exploits?
    A released malware that exposes vulnerabilities of a program before a patch can be made for it

20. By what percentage did zero-day exploits decline in 2018?
    Declined 4% from 27% in 2017 to 23% in 2018

21. What are two techniques that worms such as Emotet and Qakbot use?
    Living off the land attacks and supply chain attacks

22. What are supply chain attacks? By how much did they increase in 2018?
    Exploit 3rd party services and software to compromise final targets, hijacking updates and injecting malicious code into legitimate software. 78% increase in 2018

23. What challenge do supply chain attacks and living off the land attacks highlight for organizations?
    The attacks arrive through trusted channels using fileless attack methods or legitimate tools for malicious use

24. The 20 most active groups tracked by Symantec targeted an average of how many organizations between 2016 and 2018?
    55 organizations on average

25. How many individuals or organizations were indicted for cyber criminal activities in 2018? What are some of the countries that these entities were from?
    49 Indictments in 2018, 18 Russian, 19 Chinese, 11 Iranian, 1 North Korean

26. When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?
    Poor configuration

27. What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?
    They share pools of memory. A successful attack on a single physical system could result in data being leaked from several cloud instances

28. What are two examples of the above cloud attack?
    Melt-down and Spectre

29. Regarding Internet of Things (IoT) attacks, what were the two most common infected devices and what percentage of IoT attacks were attributed to them?
    Routers and Connected Cameras, 75% and 15%

30. What is the Mirai worm and what does it do?
    DDoS, takes down a service, network or host machine for its intended users

31. Why was Mirai the third most common IoT threat in 2018?
    It is constantly evolving, uses 16 different expolits, adds new expolits to increase success rate for infection

32. What was unique about VPNFilter with regards to IoT threats?
    First widespread threat, ability to survive a reboot making it difficult to remove

33. What type of attack targeted the Democratic National Committee in 2019?
    unsuccessful spear-phishing attack from APT29 (Russia)

34. What were 48% of malicious email attachments in 2018?
    Malicious email attachments of office files

35. What were the top two malicious email themes in 2018?
    email disguised as notifications such as invoice or receipts and attached office files containing malicious script

36. What was the top malicious email attachment type in 2018?
    Spam

37. Which country had the highest email phishing rate? Which country had the lowest email phishing rate?
    Poland at 9,653 was the highest and Saudia Arabia at 675 was the lowest

38. What is Emotet and how much did it jump in 2018?
    Financial Trojan that infects network wide. It went up 1000%

39. What was the top malware threat of the year? How many of those attacks were blocked?
    Heur.AdvML.C, 43,999,373 attacks were blocked

40. Malware primarily attacks which type of operating system?
    Windows

41. What was the top coinminer of 2018 and how many of those attacks were blocked?
    JS.Webcoinminer, 2,768,721 attacks were blocked

42. What were the top three financial Trojans of 2018?
    Ramnit, Zbot, Emotet

43. What was the most common avenue of attack in 2018?
    Spear Fishing Emails

44. What is destructive malware? By what percent did these attacks increase in 2018?
    Destructive emails are malware that can delete files or "brick" a machine at the hackers request, attacks increased by 25% in 2018

45. What was the top user name used in IoT attacks?
    Root

46. What was the top password used in IoT attacks?
    123456

47. What were the top three protocols used in IoT attacks? What were the top two ports used in IoT attacks?
    Feluet, HTTP, HTTPS. Telnet and World Wide Web HTTP

48. In the underground economy, how much can someone get for the following?

39. What was the top malware threat of the year? How many of those attacks were blocked?
    Heur.AdvML.C, 43,999,373 attacks were blocked

40. Malware primarily attacks which type of operating system?
    Windows

41. What was the top coinminer of 2018 and how many of those attacks were blocked?
    JS.Webcoinminer, 2,768,721 attacks were blocked

42. What were the top three financial Trojans of 2018?
    Ramnit, Zbot, Emotet

43. What was the most common avenue of attack in 2018?
    Spear Fishing Emails

44. What is destructive malware? By what percent did these attacks increase in 2018?
    Destructive emails are malware that can delete files or "brick" a machine at the hackers request, attacks increased by 25% in 2018

45. What was the top user name used in IoT attacks?
    Root

46. What was the top password used in IoT attacks?
    123456

47. What were the top three protocols used in IoT attacks? What were the top two ports used in IoT attacks?
    Feluet, HTTP, HTTPS. Telnet and World Wide Web HTTP

48. In the underground economy, how much can someone get for the following?

    a. Stolen or fake identity:$0.10 - $1.50
    b. Stolen medical records:$0.10 - $35
    c. Hacker for hire:$100+
    d. Single credit card with full details:$1 - $45
    e. 500 social media followers:$2 - $6