LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Unix/Mac/Linux OS Malware

10/15/2020

Report #: 202010151030

Agenda

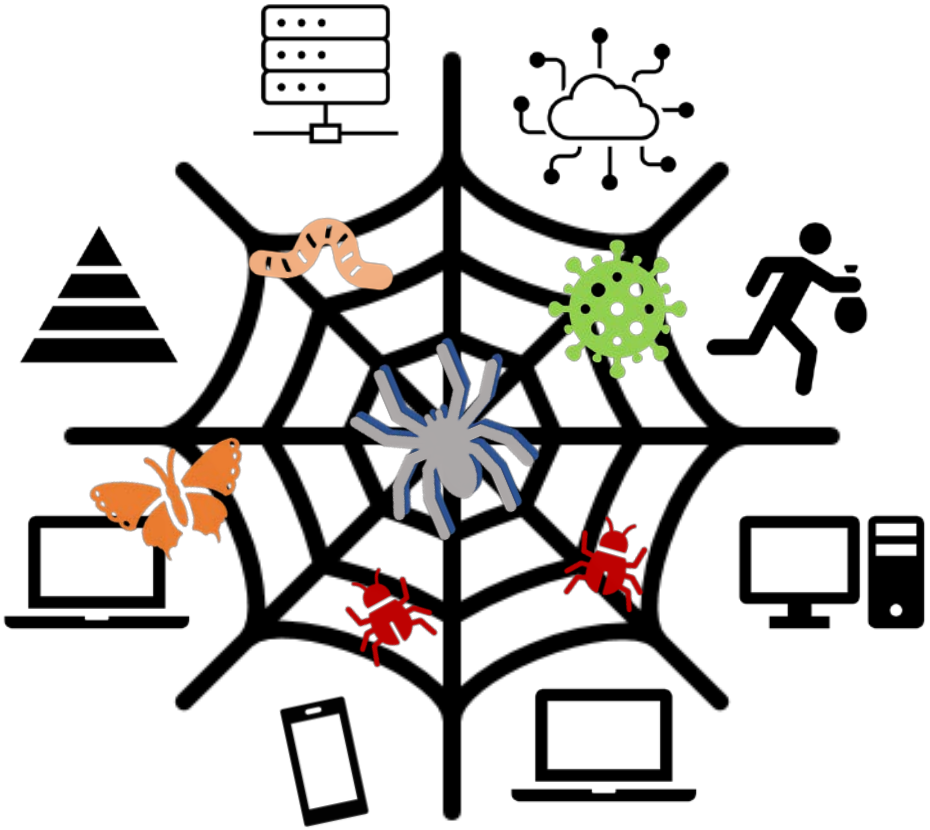
- Executive Summary
- Origin of Modern Operating Systems
- Overview of Operating Systems
  - Desktop
  - Servers
  - Super Computers
  - Mobile
  - Attack Surface and CVEs
- Malware Case Studies
  - Drovorub
  - Hidden Wasp
  - Operation Windigo
  - MAC Malware
- Defending Against Malware
- Summary

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (system admins, IRT)

- Unix and Unix-like systems drive most of today's computer systems.
- Vulnerabilities and malware
- Threat mitigation
  - Comprehensive security policies
  - Access control
  - Regular updates and backups
  - Training employees
  - Improving posture and maturity



"Determining the operating system on which the server runs is the most important part of hacking. Mostly, hacking is breaking into the target's system to steal data or any such purpose. Hence, the security of the system becomes the thing of prime importance." Source: Parikh, K. (2020, August) *The Hackers Library*

Functions of Operating Systems

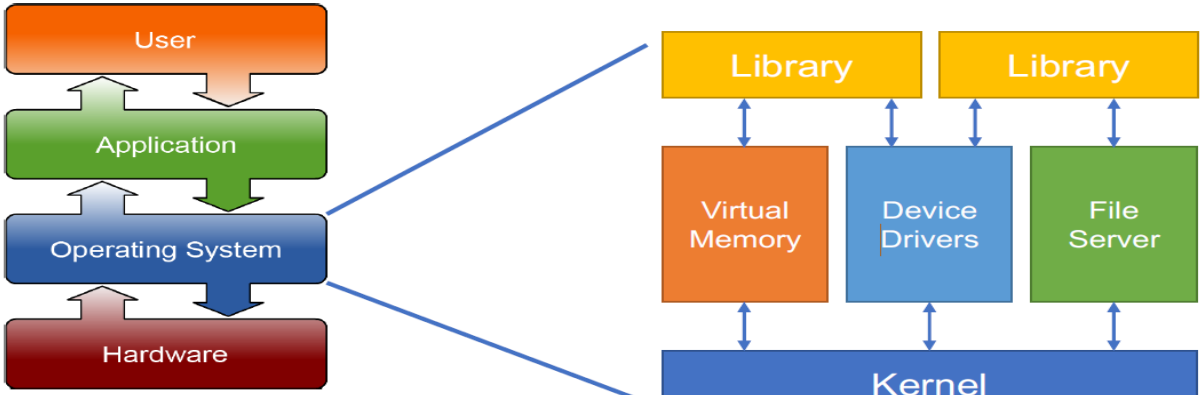
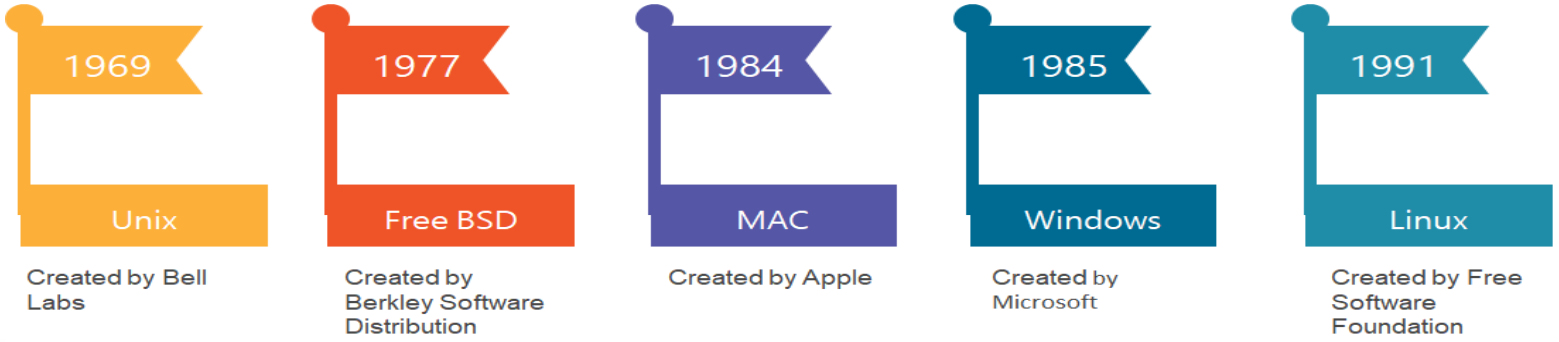


Image By Golftheman - https://commons.wikimedia.org/w/index.php?curid=4558519

Timeline of the Origins of Operating Systems



Overview of Operating Systems (Non-Mobile)

Unix
- Derived from Original AT&T Unix
- Command-line input
- Very popular among scientific, engineering and academic users
- Considered more stable than Windows
- Main frames, workstations, and supercomputers

BSD
- Free and open-source
- Based on Unix OS
- Most popular variant of BSD is Free BSD
- Not designed for personal computers
- Servers, workstations, gaming and embedded systems

macOS
- Proprietary to Apple
- Graphical user interface
- Based on Unix OS
- Second most-used OS for personal computers
- Apple computers and other products, some medical devices

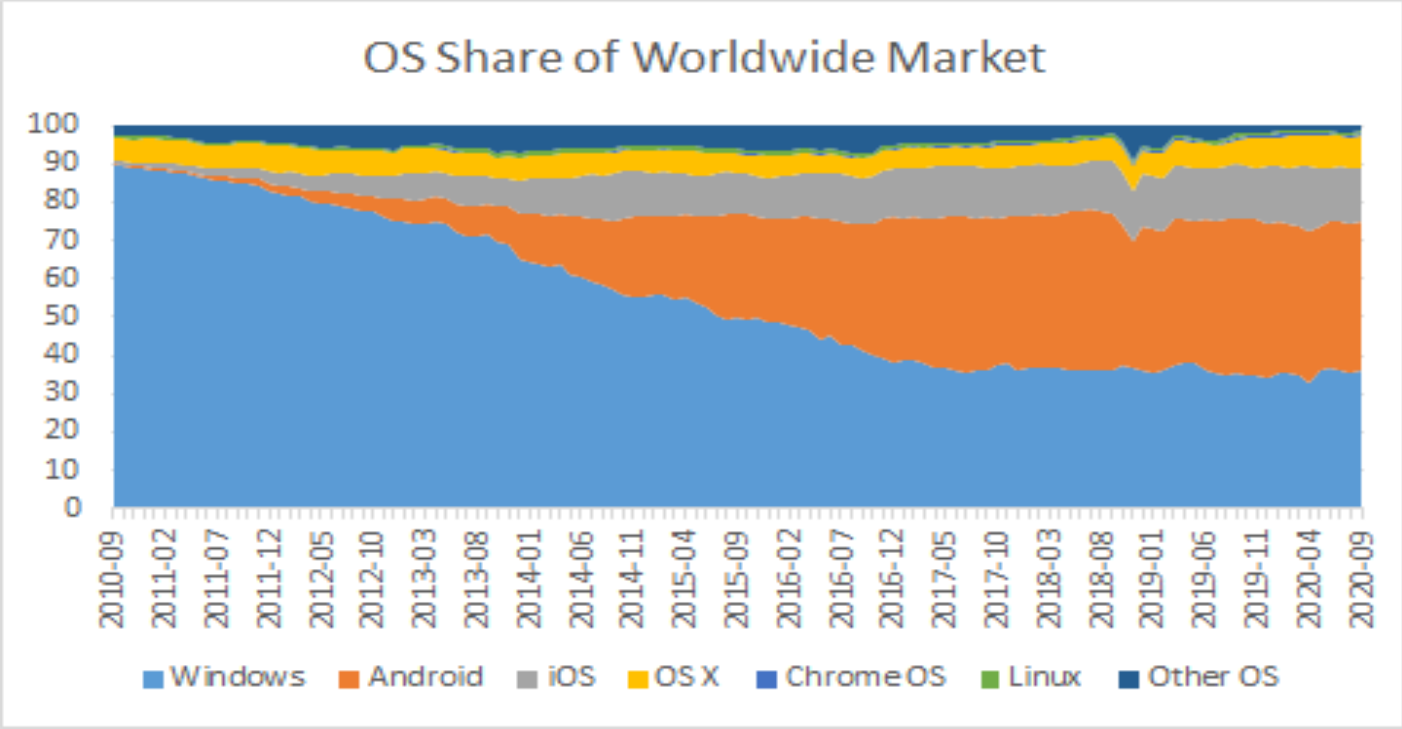
Chrome OS
- Free and open-source
- Graphical user interface
- Based on Linux
- Efficient and easy to maintain
- Chromebooks, tablets, and Google Enterprise Network

Linux
- Free and open-source, but has proprietary variants
- Command-line input
- Based on Unix OS
- More efficient than Windows
- Supercomputers, workstations, web servers, endpoint security, embedded systems

Windows
- Proprietary to Microsoft
- Graphical user interface
- Most-used OS for personal computers
- Computers, workstations, servers, endpoint security, embedded systems

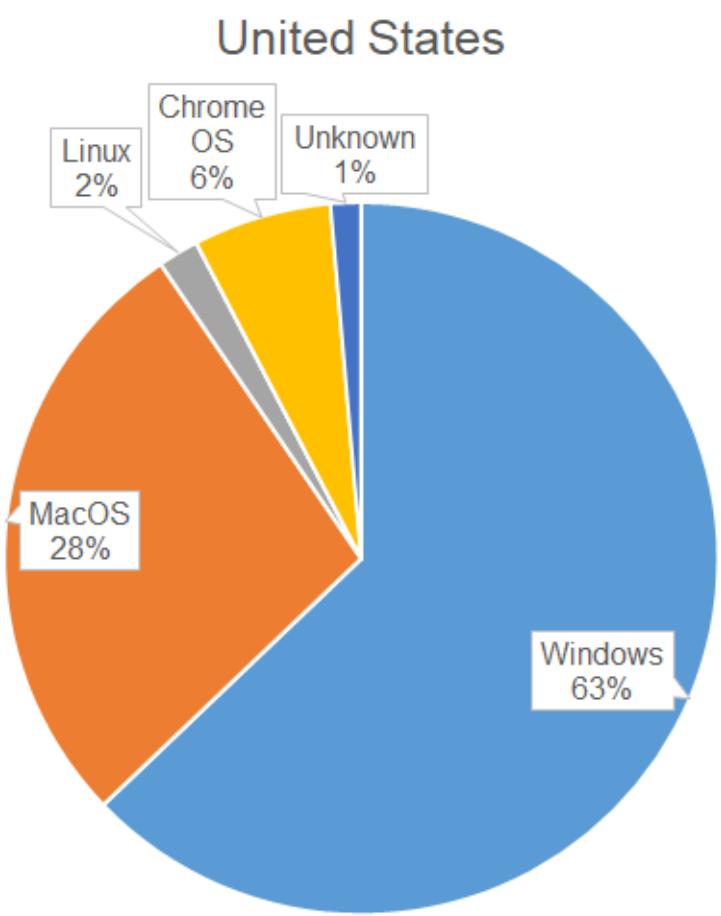
Non-Windows Attack Surfaces Have Grown

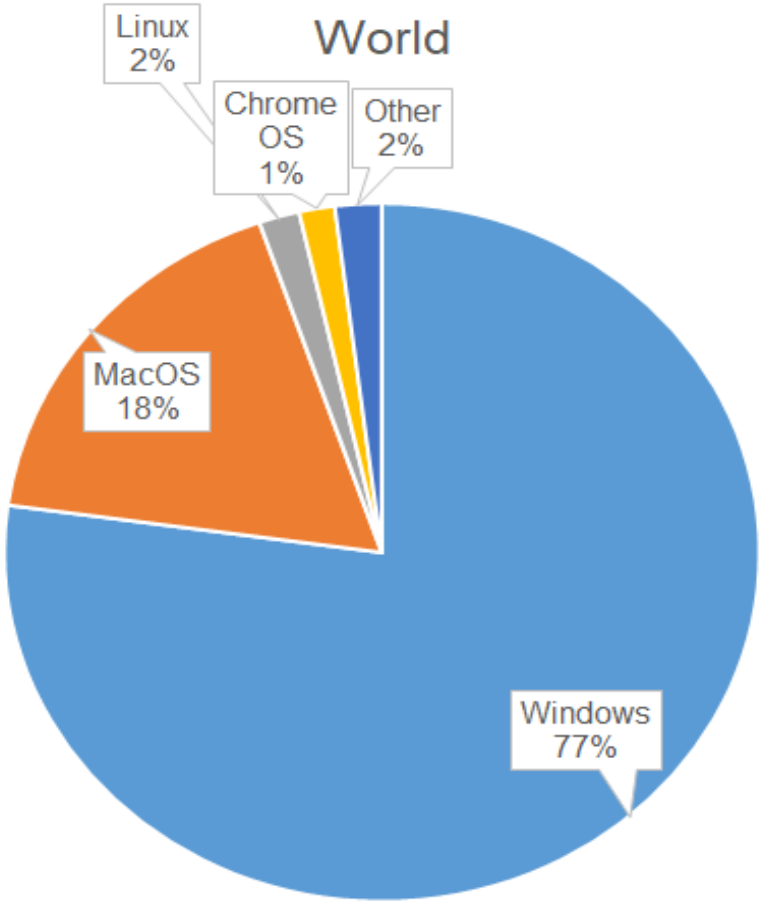
- Linux attack surfaces are growing with Linux/Unix, and BSD variants are used in about 66% of Internet web servers.
- Sales of Chromebooks, which run the Linux-based Chrome OS, grew in the U.S. by 127% between March and June 2020 compared to just 40% for Windows and Mac laptops.
- The Mobile Operating System market share is growing rapidly, as 76% of Internet users are expected to access the web solely via smartphone by 2025.



(Statcounter GlobalStats, 2020)

Operating Systems Used in Desktops/Laptops

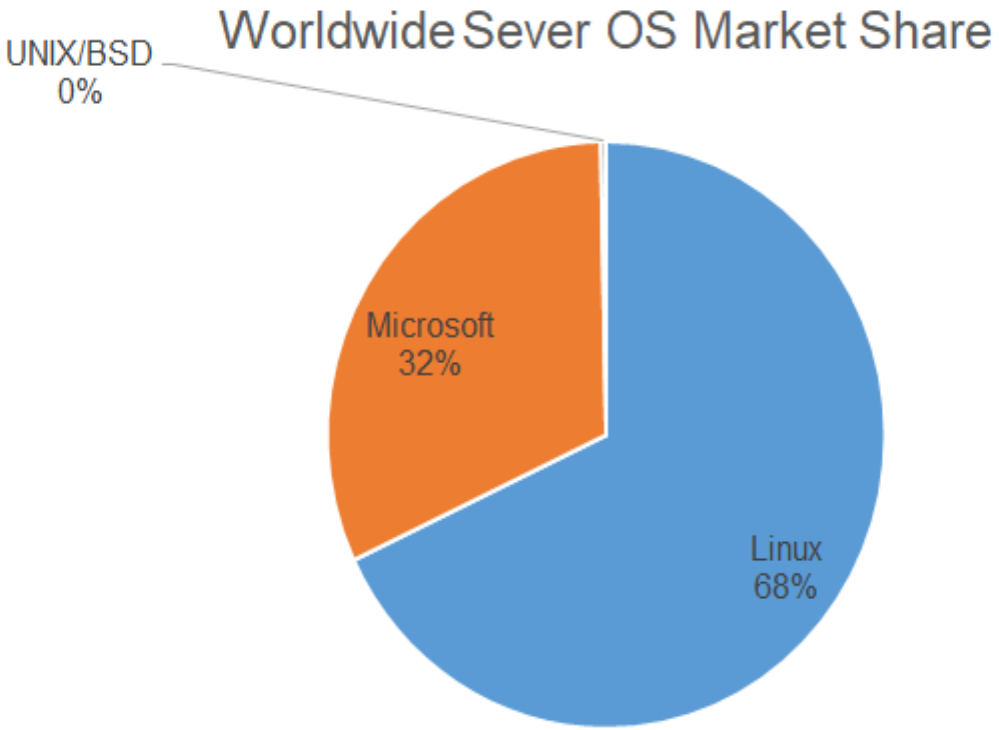




(Statcounter GlobalStats, 2020)

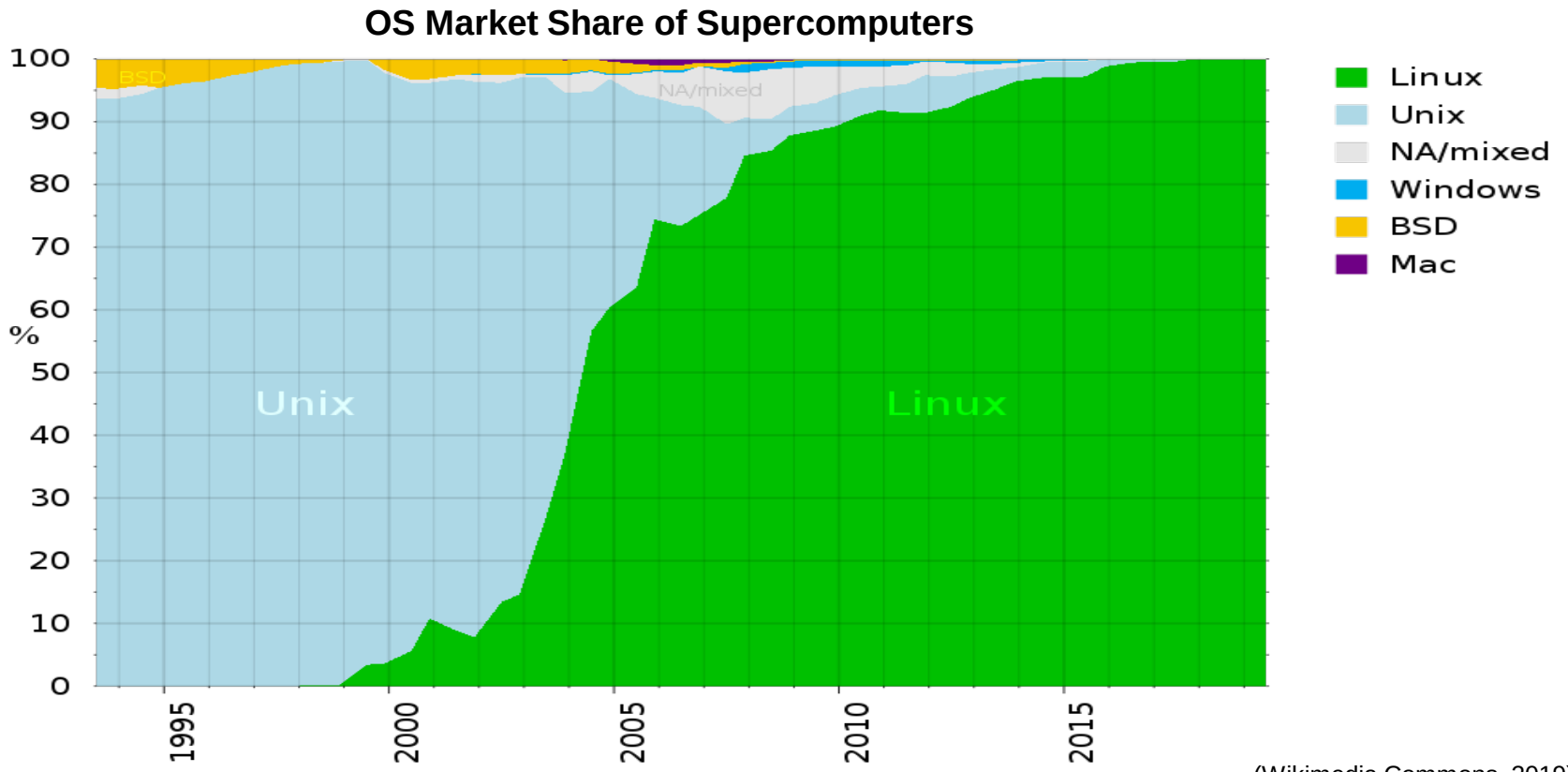
Operating Systems used in Servers

- Linux dominates the server market.
- Many web servers like Unix/BSD, Google Enterprise and Microsoft Azure Cloud use a Linux OS.
- Although Linux is free and open source, many Linux-based variants are not.
- Some paid-for variants include: Red Hat, CentOS and Gentoo. The variants Ubuntu and Fedora are free. Debian has a free version and a paid-for version.



(Team, 2018) Source: Worldwide Operating Systems and Subsystems Market Shares, 2017, IDC, 2018 #U44150918

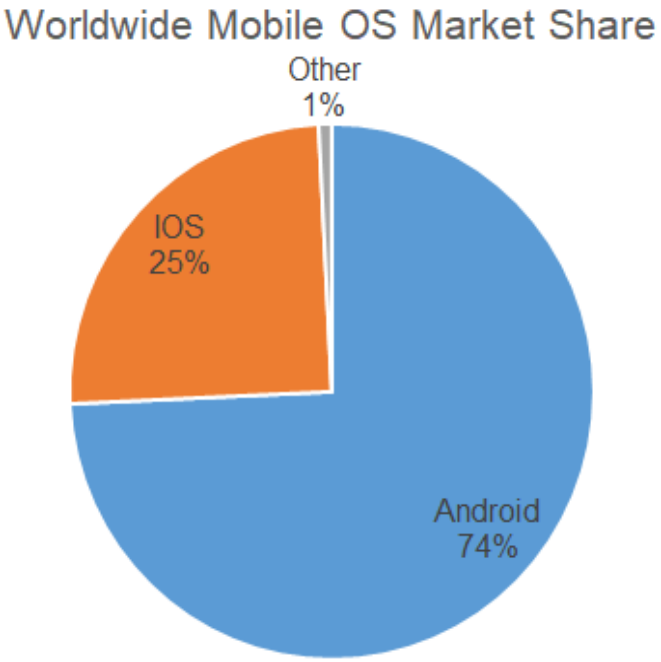
- Linux-based operating systems account for almost 100% of the supercomputer market; a market formerly dominated by Unix operating systems.

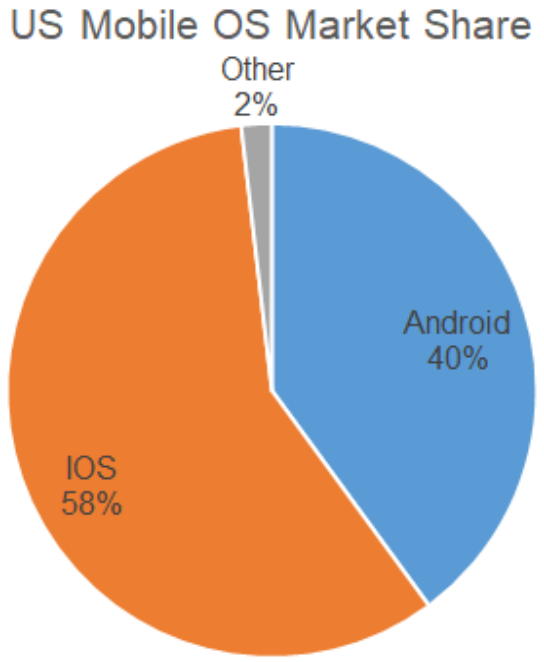


(Wikimedia Commons, 2019)

Mobile Operating Systems

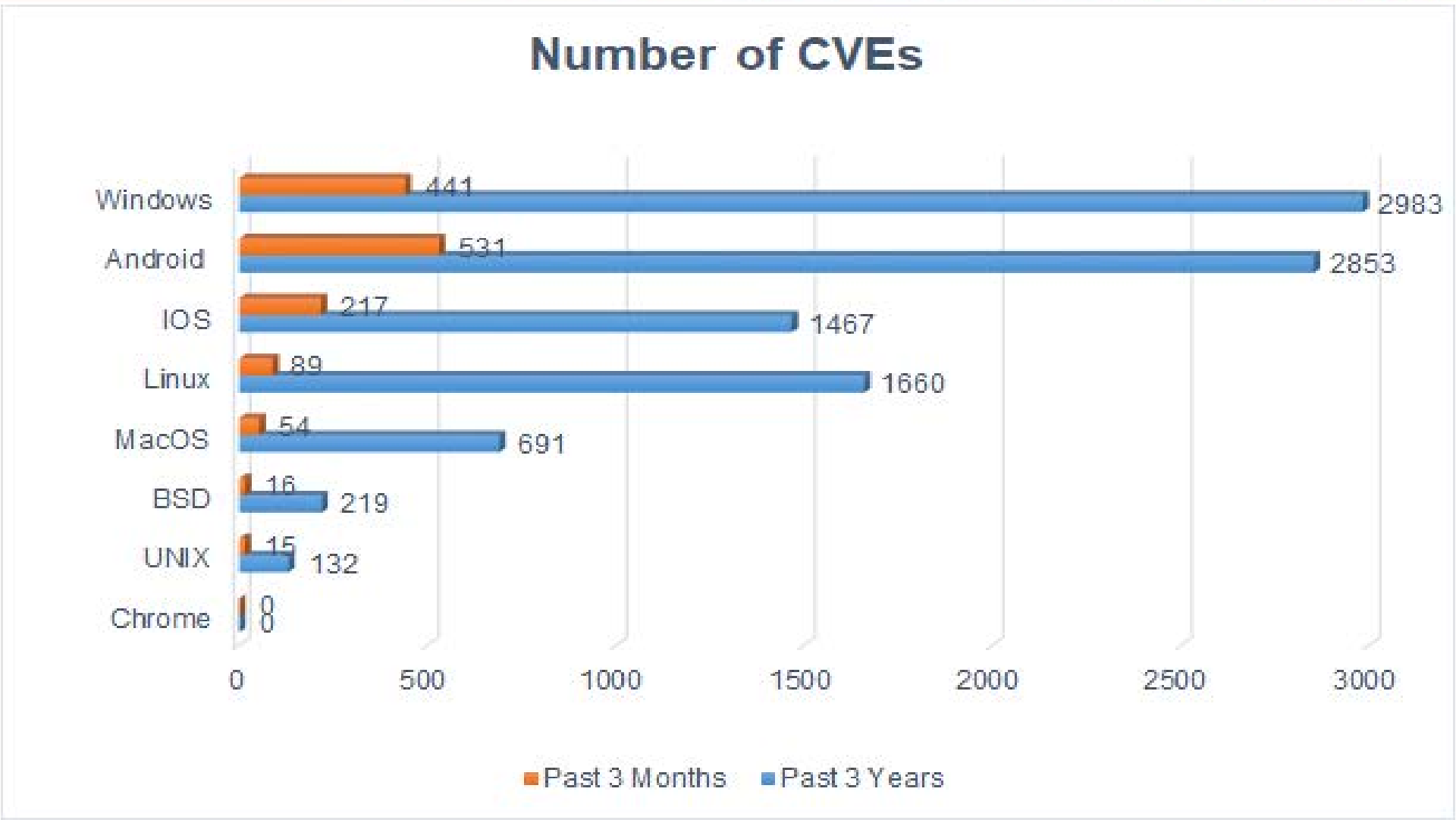
Android	IOS
• Established in 2008 • Google and the Open Handset Alliance • Open source • Based on the Linux kernel	• Established in 2007 • Apple • Proprietary • Based on Apple's Darwin, a Unix and BSD variant



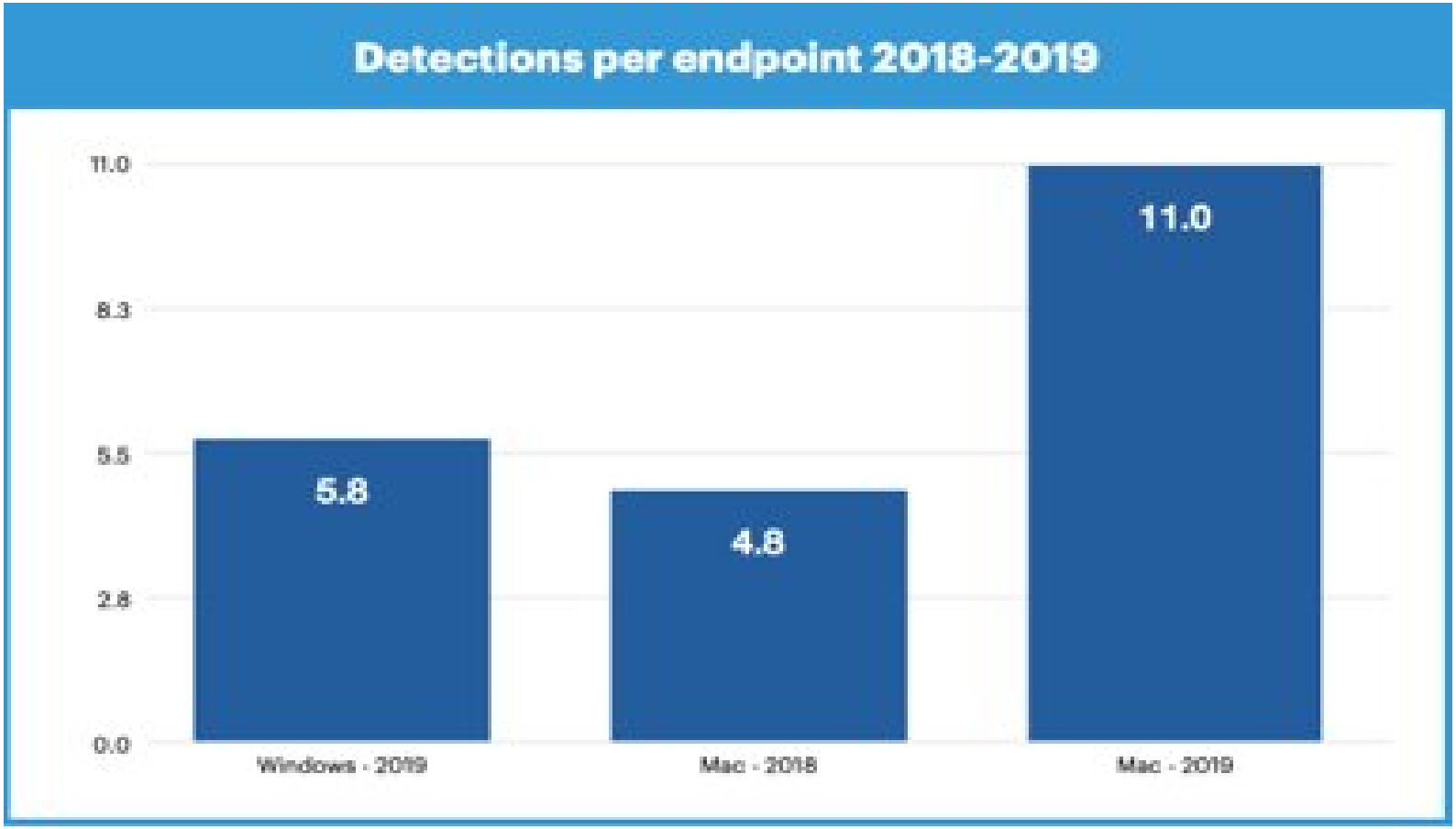


(Statcounter GlobalStats, 2020)

Linux/Unix-based OS Common Vulnerabilities and Exposures (CVE) Exceed Windows

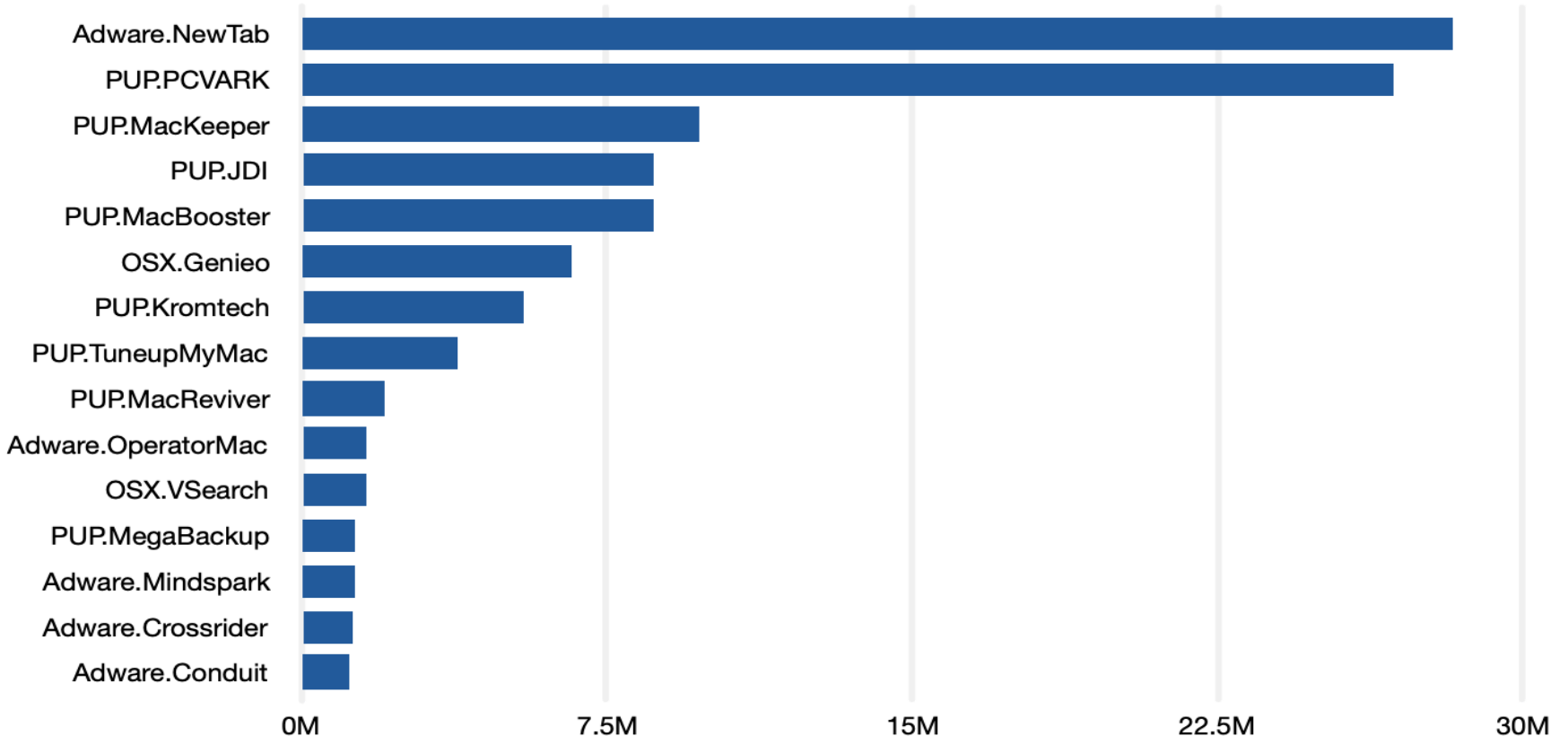


(National Institute of Standards and Technology, 2020)



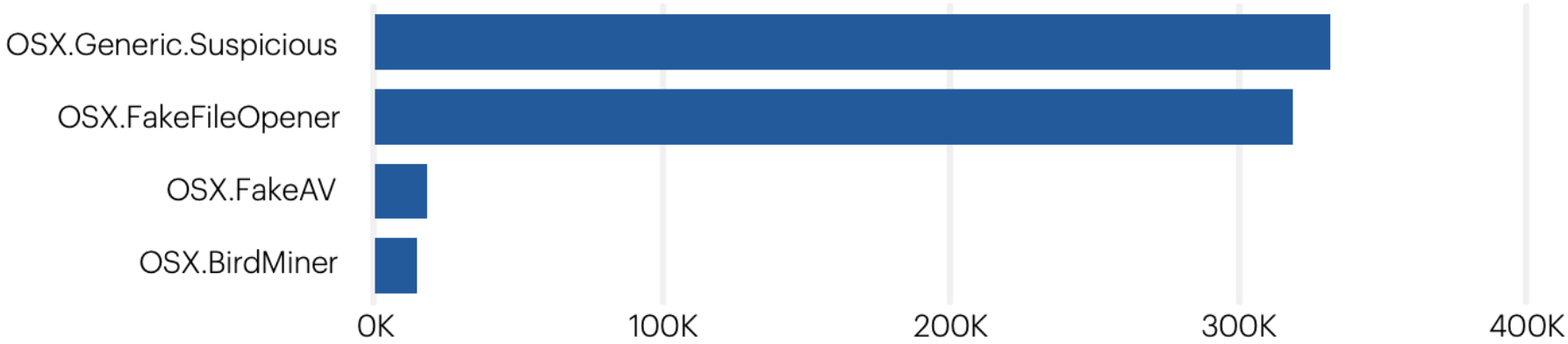
Malwarebytes 2020

Top Mac detections 2019



Malwarebytes 2020

Top Mac Malware Detections 2019



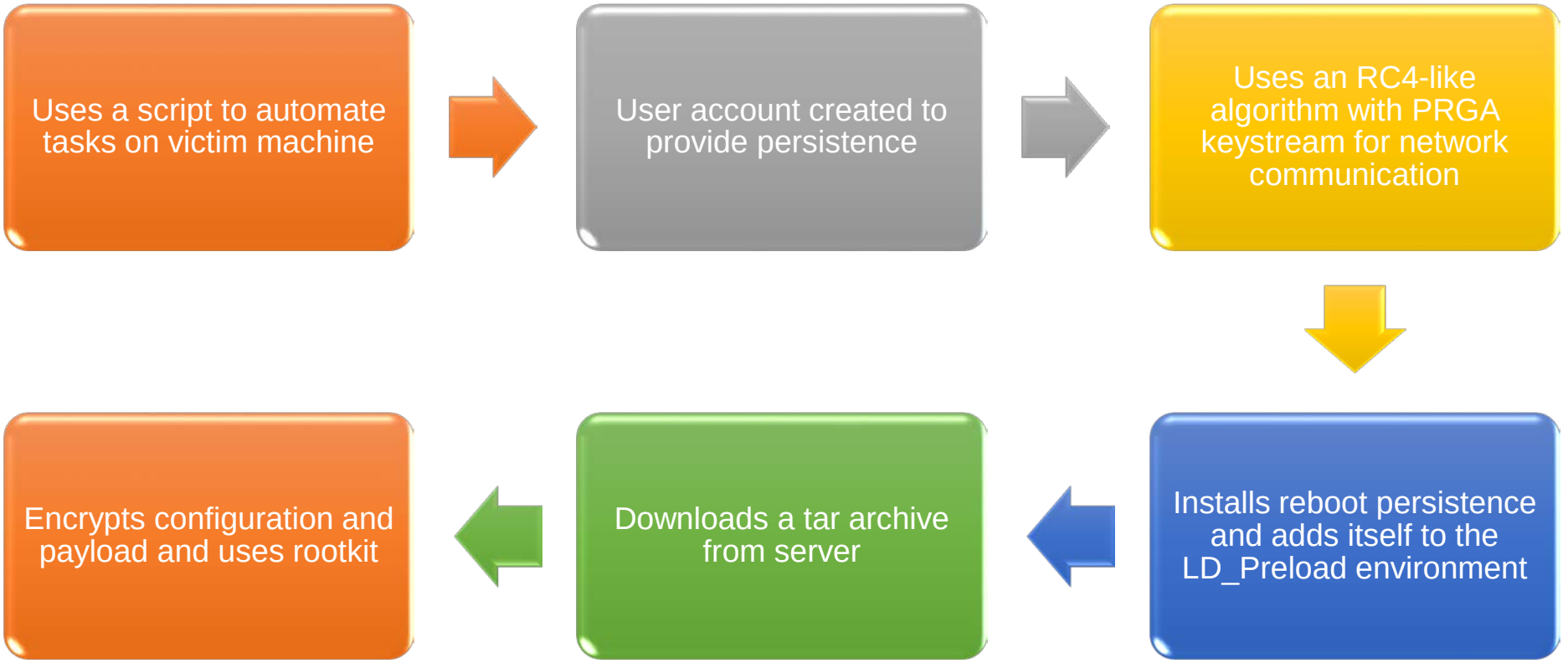
Malwarebytes 2020

iOS

- Nation-state malware, such as NSO Group's Pegasus spyware
- Zero-day vulnerability: Checkm8

Malware Case Study: Hidden Wasp

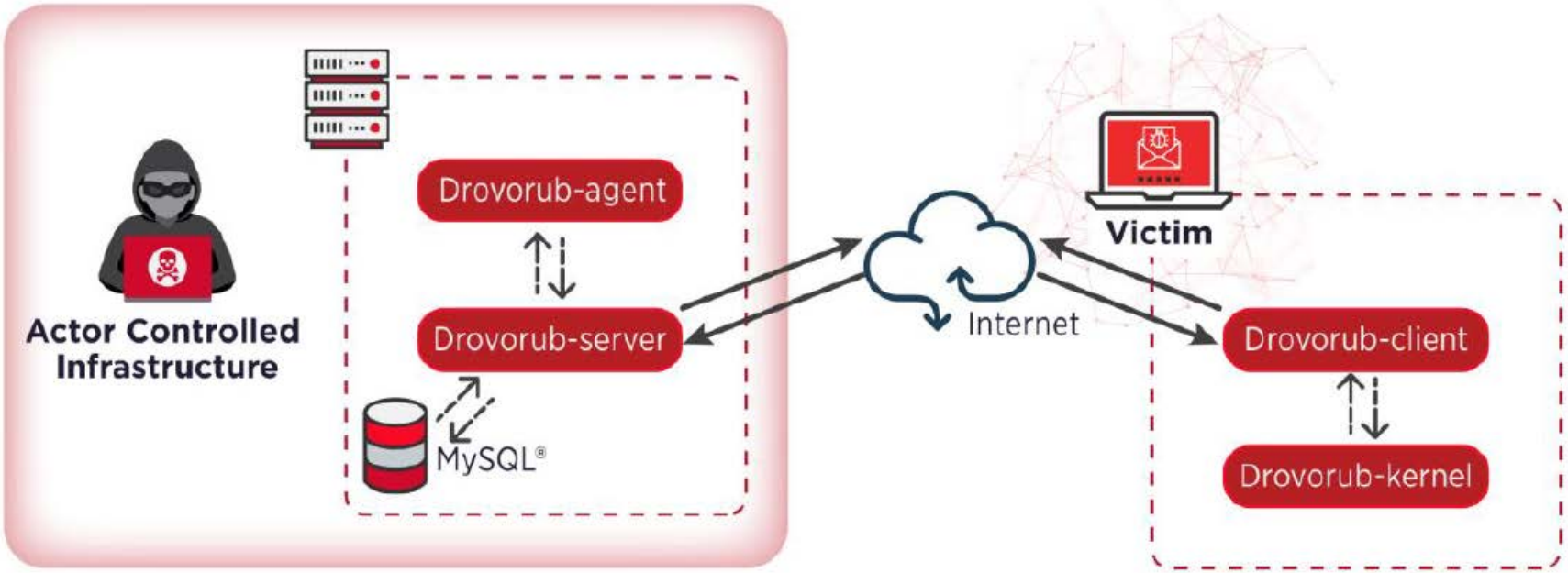
Malware Case Study: Hidden Wasp



Malware Case Study: Drovorub

- Linux malware attributed to Russian military group APT28
- Requires the attackers to gain root privileges using another vulnerability before successful installation
- Consists of an implant, rootkit, C&C server and a file transfer and port forwarding tool
- Persists through a reboot of an infected machine

Malware Case Study: Drovorub



National Security Agency 2020

Malware Case Study: Operation Windigo

- Windigo Suite (Ebury, Cdorked, Onimiki and Perl/Calfbot):
  - Disable direct root login in your OpenSSH daemon
  - Disable password-based logins and use an SSH key
  - Use multi-factor authentication on your servers
  - Use SSH agent forwarding from server to server instead of copying your SSH private keys on servers
    - On GNU/Linux, use SSH-agent
    - GNOME Keyring with ForwardAgent under a trusted host entry in your .ssh/config file6
    - On Windows, PuTTY's Pageant supports SSH agent forwarding
- Use an up-to-date antivirus solution

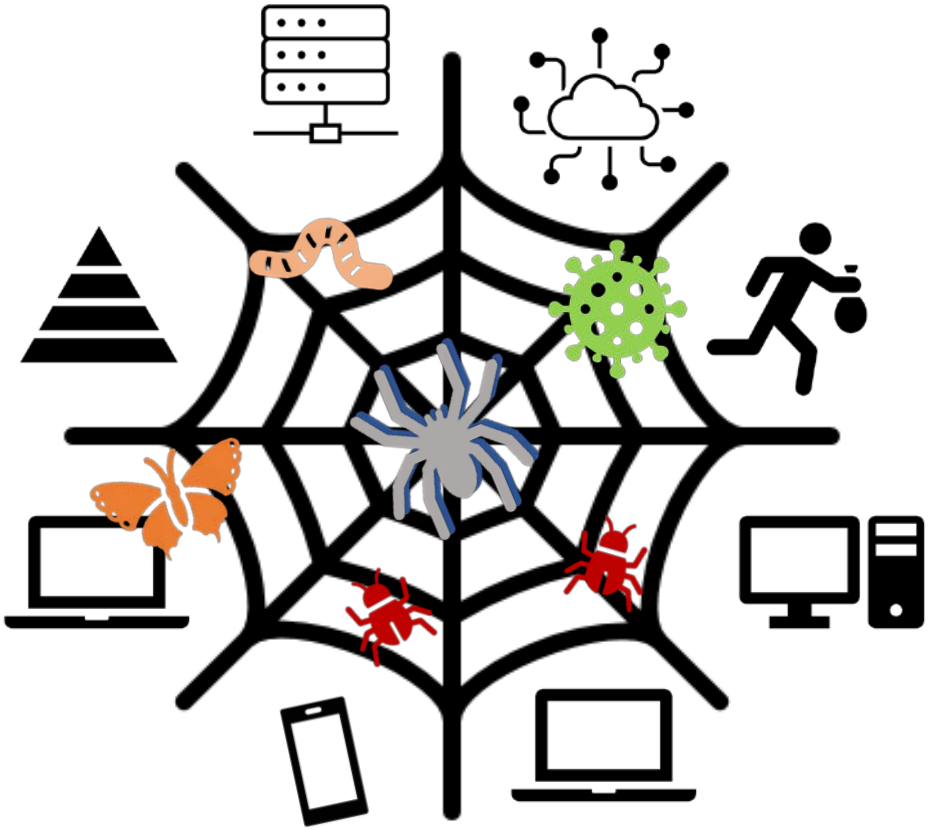
Recommendations and Mitigations

- Apply system updates to:
  - Operating system
  - Programs
  - All browsers
- Properly configure network detection and prevention systems/devices/firewalls/proxies
- Prevent untrusted kernel modules and load only modules with a valid digital signature
- Utilize a combination of system-hardening techniques and network-based controls
- Update Mac cybersecurity or anti-malware program from a reputable vendor
- Common tools such as rkhunter and chrootkit may be used to detect Linux rootkits
- Application control and software restrictions tools such as SELinux, KSPP, grsecurity MODHARDEN, and Linux kernel-tuning can aid in restricting kernel module loading
- Limit access to the root account and prevent users from loading kernel modules and extensions through proper separation
- Limit privilege escalation opportunities
- Restrict web-based content

- Restrict PowerShell execution policy to administrators
- Block Command-and-Control IP addresses
- Use multifactor authentication for user and privileged accounts
- Limit the use of local administrator accounts
- SSL/TSL inspections to see the contents of encrypted sessions and look for network-based indicators
- Restrict file and directory permissions
- Do not allow loading of remote DLLs and enable Safe DLL Search Mode
- Ensure proper registry permissions are set

Summary

- Unix and Unix-like systems drive most of today's computer systems
- Vulnerabilities and malware
- Threat mitigation
  - Comprehensive security policies
  - Access control
  - Regular updates and backups
  - Training employees
  - Improving posture and maturity



Reference Materials

References

Arghire, I. (2020, August 14). *FBI, NSA Share Details on New 'Drovorub' Linux Malware Used by Russia*. Retrieved September 2020, from Securityweek.com: https://www.securityweek.com/fbi-nsa-share-details-new-drovorub-linux-malware-used-russia

ATR Operational Intelligence Team. (2020, August 13). *On Drovorub: Linux Kernel Security Best Practices*. Retrieved September 2020, from McAfee.com: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/on-drovorub-linux-kernel-security-best-practices/

Bilodeau, O. B.-M.-J.-É. (2014). *OPERATION WINDIGO.* Bratislava, Slovakia: ESET.

Covey, L. (2019, June 14). *HiddenWasp Malware Targets Specific Linux Device Owners*. Retrieved September 2020, from Eeweb.com: https://www.eeweb.com/hiddenwasp-malware-targets-specific-linux-device-owners/

DETECTION CONTENT: DROVORUB MALWARE. (n.d.). Retrieved September 2020, from Socprime.com: https://socprime.com/blog/detection-content-drovorub-malware/

ESET. (2013, April 26). *Linux/Cdorked.A: New Apache backdoor being used in the wild to serve Blackhole*. Retrieved September 2020, from Welivesecurity.com: https://www.welivesecurity.com/2013/04/26/linuxcdorked-new-apache-backdoor-in-the-wild-serves-blackhole/

GeeksforGeeks. (2020, June 7). *Difference between Windows and Chrome OS*. Retrieved from GeeksforGeeks: https://www.geeksforgeeks.org

Hiddenwasp. (2020, March 26). Retrieved September 2020, from Attack.MITRE: https://attack.mitre.org/software/S0394/

Jerzewski, M. (2020, August 20). *The State of Security*. Retrieved September 2020, from Tripwire.com: https://www.tripwire.com/state-of-security/featured/drovorub-malware/

Koch, M. (2015). *An Introduction to Linux-based malware.* SANS Institute .

References

Kumar, M. (2014, March 18). *Operation Windigo: Linux malware campaign that infected 500,000 Computers Worldwide*. Retrieved September 2020, from Thehackernews.com: https://thehackernews.com/2014/03/operation-windigo-linux-malware.html

Lee, J. (2015, August 31). *3 Unix-Like Operating Systems That Aren't Linux.* Retrieved from Makeuseofus: https://makeuseofus.com

Malwarebytes Labs. (2020). *2020 State of Malware Rport.* Malwarebytes. Retrieved September 2020, from http://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf

Milenkovic, J. (2020, February 14). *Operating System Market Share - Bill Gates is Still Alone at the Top.* Retrieved from Kommando Tech: www.kommandotech.com/statistics/operating-system-market-share/

MITRE. (2020, September 30). *CVE Common Vulnerabillities and Exposures*. Retrieved from cve.mitre.org: https:cve.mitre.org

M.Léveillé, M.-E. (2017, October 30). *ESET research team assists FBI in Windigo case – Russian citizen sentenced to 46 months*. Retrieved Septmeber 20, from welivesecurity.com: https://www.welivesecurity.com/2017/10/30/esets-research-fbi-windigo-maxim-senakh/

National Institute of Standards and Technology. (2020, September 30). *National Vulnerability Database*. Retrieved from Vulnerabilities, Search and Statistics: https://nvd.nist.gov/vuln/search

National Security Agency, Federal Bureau of Investigation. (August 2020). *Cybersecurity Advisary: Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware.* Washington, DC: Federal Bureau of Investigation.

Olivier Bilodeau • Pierre-Marc Bureau • Joan Calvet Alexis Dorais-Joncas • Marc-Étienne M.Léveillé. (2014). *Operation Windingo: The vivisection of a large Linux server-side.* Enjo Safer Technology (ESET).

References

Parikh, K. (2020, August). *Footprinting and Reconiassance - Determining the Operating System*. Retrieved from The Hackers Library: https://libraryofhacks.blogspot.com/2017/02/footprinting-and-reconnaissance_13.html

Sanmillan, I. (2019, May 29). *HiddenWasp Malware Stings Targeted Linux Systems.* Retrieved from Intezer: https://www.intezer.com/blog/linux/hiddenwasp-malware-targeting-linux-systems/

Software. (2020, June 30). Retrieved September 2020, from Attack.MITRE: Attack.mitre.org/software/S0394

Sriram Subramanian. (2017). *Source: Worldwide Operating Systems and Subsystems Market Shares.* IDC, 2018 #U44150918.

Statcounter GlobalStats. (2020, September 30, 2020). *Desktop Operating System Market Share Worldwide*. Retrieved from statcounter GlobalStats: https://gs.statcounter.com

Team, R. H. (2018, October 2). *Red Hat continues to lead the Linux server market*. Retrieved from Redhat.com: https://www.redhat.com/en/blog/red-hat-continues-lead-linux-server-market

Techniques. (2020, June 30). Retrieved September 2020, from Attack.MITRE: https://attack.mitre.org/techniques/T1547/

Tozzi, C. (2020, September 2020). *Know Your "Nixes: Guide to Unix-Like OPerating Systems that Matter Todayt.* Retrieved from Sweetcode: https://sweetcode.io/your-nixes-operating-system/

Velázquez, L. (2019, March 21). *How to use SSH properly and what is SSH Agent Forwarding*. Retrieved from Dev.to: https://dev.to/levivm/how-to-use-ssh-and-ssh-agent-forwarding-more-secure-ssh-2c32

Wikimedia Commons. (2019, June 17). *Operating systems used on the top 500 supercomputers.* Retrieved from Wikimedia Commons: https://commons.wikimedia.org

Questions

Upcoming Briefs

- Next briefing
- Awesome upcoming material

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.

HC3 Customer Feedback

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.
Visit us at: www.HHS.Gov/HC3

Contact

www.HHS.GOV/HC3

(202) 691-2110

HC3@HHS.GOV