Cyber Law
Group #4

Cyber Incident: ROT Polymorphic Worm

By Alex Turnsek, Cara O'Toole, Eric Preston, Shekhinah Green, Steve Day, Ayoob Ibrahim, Noah Canody and Xavier Jasper

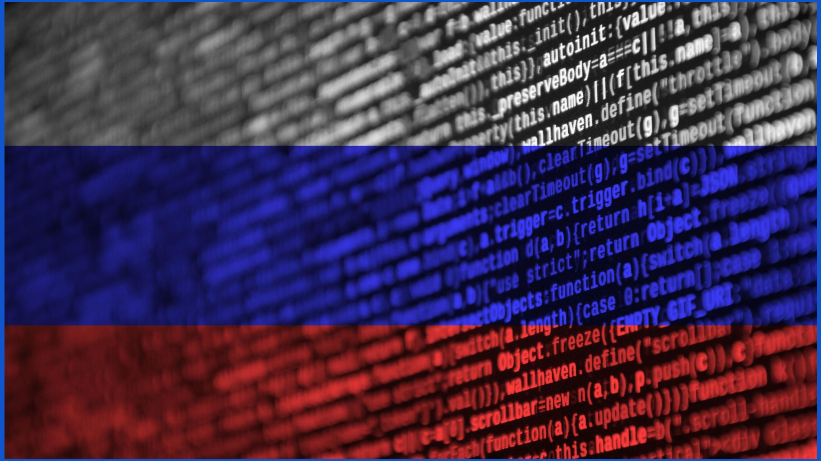
What Happened?

- A polymorphic worm had breached Apple’s systems via a malicious email and spreading through an update, compromising the PII and bank accounts of most American citizens as well different areas of critical infrastructure.
- The worm utilized a powerful stolen tool from the NSA to breach Apple’s systems but still be contained enough to only affect our country. It would also create a backdoor on any device it compromised to extract the needed information.

Who's Responsible?

On the first day of the attack, the worm was contained but at the cost of compromising and damaging a significant number of devices.

After some digging into the worm's code and metadata, it appears to be of Russian origin from a criminal organization that is heavily connected to the Russian government.



Consequences/Damage Dealt

- Billions of dollars for the number of damaged Apple devices and different areas of infrastructure significantly damaged
- Data leakage of hundreds of millions of citizens due to the rapid spread of the worm
- Severely halted people's access to the internet due to network infrastructure being damaged
- Compromised critical infrastructure such as hospitals, energy, and finance.

Incident Management Agencies

Executive Office of the President - Plays the role of national response after the initial attack to determine the best course of action with the support of other agencies.

DHS - A significant coordinator with the President, managing federal agencies, and working with FEMA

CISA - Collaborates with the DHS for asset and incident response as well as coordinating with the public and private sector affected companies

FBI - The lead investigative force in collaboration with the DOJ and other agencies.

NSA - Focuses on containment of the worm as well as using other tools to understand the circumstances

DOJ - The National Security and Criminal Divisions would be working to establish the legal action against the criminal organization

DoD - Would be the first line of defense for the attack, utilizing the Defend Forward strategy and supporting the FBI's investigation

DOS - Connects with foreign governments to alert them and learn if the worm spread outside of the U.S.

Responding Agencies

FBI’s National Cyber Investigative Joint Task Force (NCIJTF) - Collects evidence in order to begin establishing attribution

CISA - Sends out teams of cyber security experts and utilizes the NCIRP

DoD’s Cyber Command - Utilized to protect critical federal assets via collaboration with agencies

DOJ - Would support the FBI in its investigation along with legally support the afflicted companies

FEMA - Collaborating with critical infrastructure companies and the DHS to mitigate their damage

NSA - Analyzes the malware and develop a solution to get networks back to previous operations

Private Sector Companies - Companies involved in critical infrastructure, as well as affected by the initial attack

Response Weaknesses

- Extended response time of Agencies and Apple to communicate updates
- Too many cybersecurity professionals were stretched to their limit with the attack
- The initial attack caused communications problems between agencies

Response Corrections

- Have the Executive Office create concern relief response for the public for greater transparency.
- Invest in more cybersecurity professionals within federal agencies and national-level exercises
- Foster collaboration with the DHS and NSA to develop a national incident response plan.

Clarifications or Questions?

References

https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2025/01/15/fact-sheet-new-executive-order-on-strengthening-and-promoting-innovation-in-the-nations-cybersecurity/

https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

https://www.cisa.gov/sites/default/files/2025-01/NCIRP%20Update%20Public%20Comment%20Draft%20508c__0.pdf

https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia#:~:text=Organizations%20should%20report%20anomalous%20cyber,to%20warn%20other%20potential%20victims.

https://www.cisa.gov/topics/cybersecurity-best-practices/organizations-and-cyber-safety/cybersecurity-incident-response#:~:text=When%20cyber%20incidents%20occur%2C%20the,nation%20response%20to%20cyber%20incidents.

https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity#:~:text=If%20companies%20decide%20not%20to,the%20government%20and%20individual%20companies.

https://www.cybercom.mil/Components/

https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/

https://www.fbi.gov/investigate/cyber

https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force#:~:text=As%20a%20unique%20multi%2Dagency,that%20it%20coordinates%20and%20supports.

https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force

https://www.fema.gov/press-release/20231107/fema-and-cisa-release-first-ever-cyber-incidents-planning-guidance-emergency

https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global#:~:text=%E2%80%9CThe%20Department%20of%20Justice%20will,all%20the%20world%20to%20see.%E2%80%9D

https://www.nsa.gov/Cybersecurity/Overview/

https://www.nsa.gov/Portals/75/documents/what-we-do/cybersecurity/nscap/NSCAP%20Accredited%20Companies_06042019.pdf?ver=2019-08-07-110332-497

https://www.state.gov/cybersecurity/#:~:text=The%20DSS%20Foreign%20Affairs%20Cybersecurity,expedite%20internal%20threat%20mitigation%20actions