THE TYPICAL DATA BREACH TAKES AN AVERAGE OF 212 DAYS TO BE DETECTED.[1] YOU CAN DO BETTER.

THE 5 PILLARS
OF SECURITY

While hackers can lurk in systems for a long time, Managed Detection and Response solutions can work quickly to protect your systems and information. This timeline shows a real-world example of an incident and response by MDR experts. Learn how we can help.

Compromise, Investigation, and Response Timeline

Healthcare Attack Breakdown

Threat
Solarmarker
Jupyter infoStealer
Yellow Cockatoo

Type
Persistence -
Run Key Added by Reg.exe

Severity
High

Alert Priority:
Medium

Event Source
Process Start Activity

Attacker Activity

- [User1] searches "employee handbook of pharmaceutical employees" on Edge browser, unknowingly downloads document with malicious payload.
- Payload executes on [Host1], creating hundreds of decoy files in the same directory as executable to act as persistence mechanism and hide the malicious file.
- Executable file attempts to communicate with unknown Command and Control (C2) to post information about the asset and exfiltrate more data.

00:01:43 **ALERT: ATTACKER ACTIVITY DETECTED**

Rapid7 MDR detects run keys being added to the registry on machine in the customer's environment, triggering investigation.

00:06:47 **Investigation Begins**

Rapid7 SOC analyzes attacker activity (including all decoy files) using available forensic data. Confirms attack contains advanced deception techniques associated with Solarmarker/Jupyter infoStealer/Yellow Cockatoo family of malware.

Active Response and Initial Notification

MDR Analyst kicks off Active Response automation workflows to quarantine [Host1] and disable [User1]'s compromised account. Containment actions initiate after customer's 10:00 acknowledgment grace period.

MDR notifies customer of the incident and suggests additional actions to block the Indicators of Compromise (IOCs).

00:10:00 **ATTACKER CONTAINED**

Customer Takes Action
Customer takes additional remediation and mitigation recommendations.

Customer Advisor Reaches Out
Rapid7 Customer Advisor calls to follow up, ensure initial remediation actions are taken, and answer questions while Final Incident Report is developed.

BUILDING RESILIENCE

Forensic Investigation

SOC Analyst begins Digital Forensics and Incident Response (DFIR) analysis to determine full attacker timeline and actions for Final Incident Report.

Final Report Delivered
Detailed analysis, investigation synopsis, and evidence with additional recommendations.

REMEDIATION:
- Rebuild affected systems
- Block malicious domains
- Block malicious IP addresses
- Change passwords for affected accounts

MITIGATION:
- Implement least-privilege for all users
- User awareness training
- Review firewall and proxy policies
- Disable ingress access to remote administration solutions from non-VPN addresses

CA FOLLOW UP
Customer Advisor reviews incident, response recommendations, and security posture improvements.

Image Source: https://www.rapid7.com/info/mdr/MDR-timelines-tick-tocks/

Hackers operate around the clock and across time zones and so should your security team. Establishing a Security Operations Center (SOC) demands highly skilled, specialized security experts, but few organizations can achieve this, even with unlimited resources. See how quickly a Managed Detection and Response solution can get to the who-what-when-where-why quickly with the work of Customer Advisors, practitioners with strong technical expertise.

THE 5 PILLARS
OF SECURITY

- DEVICE SECURITY
- DOCUMENT SECURITY
- PRINT SECURITY
- CYBERSECURITY
- INFORMATION SECURITY

Canon U.S.A.'s Five Pillars of Security presents a portfolio of security products and services in a comprehensive way that groups solutions in functional areas. Cybersecurity is a key component of our Five Pillar approach.

[1] *IBM Cost of a Data Breach Report, 2023.*

Canon

1-844-50-CANON | usa.canon.com/security

Canon U.S.A. does not provide legal counsel or regulatory compliance consultancy, including without limitation, regarding Sarbanes-Oxley, HIPAA, CCPA, GDPR, GLBA, Check 21 or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance. Canon products offer certain security features, yet many variables can impact the security of your devices and data. Canon does not warrant that use of its features will prevent security issues. Some security features may impact functionality/performance; you may want to test these settings in your environment. Canon is a registered trademark of Canon Inc. in the United States and elsewhere. Rapid7 is a registered trademark of Rapid7 LLC. All other referenced product names and marks are trademarks of their respective owners and are hereby acknowledged. Neither Canon Inc. nor Canon U.S.A., Inc. represents or warrants any third-party product or feature referenced hereunder.

©2025 Canon U.S.A., Inc. All rights reserved.