CONVERGE
TECHNOLOGY SOLUTIONS

THREAT INTEL REPORT 2025

Prepared by: Converge Cybersecurity Practice
convergetp.com/cybersecurity | 800.747.8585

March

Observations for March 2025

The global cybersecurity landscape is witnessing a troubling shift as governments, cybercriminals, and advanced threat actors exert increasing pressure on digital security frameworks. Apple's decision to **remove its Advanced Data Protection (ADP) feature** from iCloud in the UK following government demands for encryption backdoors highlights a growing concern over state influence on cybersecurity policies. This move sets a precedent for how governments may pressure technology providers to weaken security features, raising alarms about the broader implications for data privacy and enterprise risk management. Organizations that rely on cloud-based security features must prepare for potential disruptions as vendors navigate regulatory demands that may compromise data protection standards.

Meanwhile, the **Darcula Phishing-as-a-Service (PhaaS)** platform continues to evolve, enabling even low-skilled cybercriminals to launch highly sophisticated phishing attacks. With the release of Version 3, attackers can instantly clone legitimate websites and exploit mobile messaging platforms like RCS and iMessage to bypass traditional email security controls. The shift toward automation and real-time credential theft mechanisms signals a critical escalation in phishing threats. Businesses must act swiftly to reinforce authentication protocols, deploy advanced monitoring solutions, and educate employees on emerging phishing tactics that extend beyond email-based threats.

Further complicating the cybersecurity landscape is a newly identified phishing campaign leveraging the **ClickFix technique** to distribute the Havoc command-and-control (C2) framework through Microsoft SharePoint. By exploiting Microsoft Graph API, attackers are able to obfuscate malicious traffic, bypassing conventional detection methods. The campaign underscores the growing threat of cloud service abuse, where trusted platforms are weaponized to evade security controls. Enterprises relying on Microsoft 365 and cloud-based collaboration tools must **enhance monitoring capabilities, strengthen user awareness, and implement robust access control**s to mitigate the risks of cloud-centric attack vectors.

Executive Overview

DO WE WEAKEN OR BAIL?

Audience

- C-Suite Executives
- CISO
- IT Managers
- Risk Management Professionals
- Cybersecurity Professionals and Analysts
- Business Organizations

Apple has removed its Advanced Data Protection (ADP) feature from its iCloud service in the United Kingdom following demands from the UK government to provide backdoor access to encrypted data. The decision raises concerns over global data privacy and government influence on cybersecurity policies. While Apple has maintained a strong stance against backdoors, its withdrawal of ADP in the UK sets a precedent for how governments can pressure technology companies to alter security features.

READ MORE: TACTICAL GUIDANCE

Dracula V3: The Evolution of Phishing-as-a-Service

Audience

- CISO
- Security Managers
- Cybersecurity Professionals
- IT Engineering Teams

The Darcula Phishing-as-a-Service (PhaaS) platform continues to pose a growing threat to organizations worldwide. Its newly released Version 3 (V3) now enables fully automated phishing site generation, allowing attackers to clone any brand's website with ease. Unlike traditional phishing campaigns, this new method allows even low-skilled cybercriminals to execute highly effective attacks that evade traditional detection methods.

Organizations across all sectors, are at increased risk of impersonation and credential theft. The ability to automate phishing and leverage mobile messaging services like RCS and iMessage instead of email means traditional email-based security measures will no longer be sufficient. Companies must take immediate action to strengthen authentication mechanisms, monitor for domain impersonation, and deploy proactive detection strategies to combat this threat.

READ MORE: TACTICAL GUIDANCE

Can you help me Fix It?

Audience

- C-Suite Executives
- CISO
- Security Managers
- Cybersecurity Professionals

A newly identified phishing campaign, utilizing the ClickFix social engineering technique, has been observed distributing the open-source Havoc command-and-control (C2) framework through Microsoft SharePoint. The attack method exploits Microsoft Graph API to mask malicious C2 traffic, thereby bypassing conventional network security measures. The campaign primarily targets corporate users with phishing emails that contain HTML attachments, which, upon execution, trick victims into running PowerShell commands that establish persistence and facilitate malware deployment.

READ MORE: TACTICAL GUIDANCE

Tactical Guidance

DO WE WEAKEN OR BAIL?

OVERVIEW & IMPACT

Apple's ADP feature offers end-to-end encryption for iCloud, preventing unauthorized access—even by Apple itself. The UK government's request for decryption capabilities under the Investigatory Powers Act (IPA) highlights an ongoing tension between privacy rights and law enforcement objectives. The primary concerns stemming from this development include:

IMPACT

- **Regional Precedents:** If other vendors or SaaS providers choose to comply with government-mandated backdoors, global security standards may weaken, affecting data protection beyond the specific regions in question. This could lead to a fragmented security landscape where different regions enforce varying levels of encryption, creating operational complexities for multinational organizations. Companies that prioritize strong encryption may find themselves restricted from operating in regions with stringent compliance requirements favoring government access to encrypted data.
- **Enterprise Data Risks:** Businesses that rely on these providers may face increased exposure to compliance challenges, regulatory inconsistencies, and security threats if encryption is selectively weakened. Organizations operating across multiple regions must navigate conflicting legal obligations, ensuring they remain compliant while maintaining security best practices. Additionally, the introduction of backdoors could increase the likelihood of cybercriminals exploiting these vulnerabilities, leading to data breaches and reputational damage.
- **Operational Disruptions:** Organizations must prepare for the possibility that vendors or SaaS providers will remove essential security features to maintain their overall security posture, forcing enterprises to find alternative solutions. This shift may require organizations to reevaluate their reliance on vendor-provided security tools, invest in alternative encryption methods, or migrate to service providers that prioritize data protection. The sudden loss of critical security features could disrupt business operations, particularly for industries handling sensitive information, such as finance, healthcare, and legal sectors.

RETURN

OBSERVATIONS

- Apple opted to remove ADP rather than introduce a security backdoor, setting a precedent for companies prioritizing security over compliance.
- Other SaaS providers may face similar pressures, leading to either weakened security standards or withdrawal of critical security features in certain regions.
- Governments argue that encryption hinders law enforcement, but cybersecurity experts warn that once encryption is weakened for one entity, it becomes vulnerable to exploitation by malicious actors.
- Businesses relying on SaaS solutions must prepare for a scenario where key security features are no longer available due to vendor decisions.

GUIDANCE

Strategic Intelligence

- **Trend Analysis:** Organizations must anticipate that governments will continue to push for encryption backdoors, influencing global security policies.
- **Geopolitical Risks:** Enterprises operating in multiple jurisdictions should assess the potential for regional compliance conflicts when selecting cloud and SaaS providers.
- **Vendor Security Commitments:** Businesses should prioritize vendors with clear commitments to maintaining strong security postures despite regulatory pressures.

Operational Intelligence

- **Security Controls:** Organizations should evaluate encryption alternatives and self-managed security solutions to ensure continued data protection.
- **Regulatory Compliance:** Enterprises must assess how regional security changes impact global compliance requirements, such as GDPR and CCPA.
- **Risk Mitigation:** Business continuity planning must include contingencies for the loss of critical security features provided by SaaS vendors.

Tactical Intelligence

- **Mitigation Strategies:**
    - Establish Zero Trust Architectures to minimize reliance on third-party security features.
    - Utilize self-managed encryption where organizations control their own encryption keys.
    - Implement multi-cloud redundancy to avoid dependence on a single vendor's security policies.
- **Contingency Planning:**
    - **If Vendors Weaken Security:**
        - Assess and document which services rely on vendor-managed encryption.
        - Deploy additional encryption layers to mitigate security risks.
        - Consider migrating sensitive workloads to vendors committed to strong security policies.

RETURN

- **If Vendors Remove Critical Features:**
  - Identify alternative solutions that maintain security and operational efficiency.
  - Engage in contracts that outline vendor commitments to long-term security support.
  - Develop an internal encryption and data protection strategy that reduces reliance on external providers.

THREAT HUNTING HYPOTHESES

N/A

Sources

- **Privacy International:** Apple and the Long Secret Arm of the UK Government
- **TechRepublic:** Apple Advanced Data Protection Removed in the UK
- **Apple Support:** Understanding Advanced Data Protection
- **PCMag:** Apple Halts Advanced Data Protection Feature in UK Over Encryption Feud
- **The Verge:** Apple Removes Encryption Advanced Data Protection in UK
- **The Guardian:** Apple Removes Advanced Data Protection Tool in UK
- **CyberPeace: Privacy vs. Regulation:** Apple's Advanced Data Protection Rollback in the UK
- **Privacy Guides:** UK Forced Apple to Remove Advanced Data Protection

DARCULA V3: THE EVOLUTION OF PHISHING-AS-A-SERVICE

OVERVIEW & IMPACT

With Darcula V3, the phishing landscape has changed drastically. The ability to clone any website on demand gives attackers the ability to bypass many security defenses and social engineering training programs. Organizations must recognize that brand trust and customer confidence are at stake. Attackers no longer need pre-made templates—they can instantly generate phishing kits impersonating any brand, leading to a surge in phishing campaigns.

IMPACT

- **Brand Impersonation at Scale:** Any brand, from global corporations to small businesses, can be easily mimicked.
- **Automated Credential Theft:** The platform supports real-time data collection and stolen credential notifications via Telegram.
- **Financial Fraud Capabilities:** Integration with digital wallet generation allows stolen credit card data to be converted into usable virtual cards.
- **Growing Cybercriminal Adoption:** With 400+ active users in private Telegram groups and a rapid increase in domain registrations, Darcula is expanding its reach.

OBSERVATIONS

- **Shift from Email to Mobile-Based Phishing:** Attackers now rely on RCS/iMessage phishing instead of email, making existing security training and phishing detection models outdated.
- **Sophisticated Anti-Detection Features:** Darcula V3 includes IP blocking, user-agent filtering, and randomized URL paths to bypass security monitoring.
- **Instant Cloning of Targeted Brands:** Cybercriminals no longer need pre-existing phishing kits; they can enter a URL and generate a phishing kit instantly.
- **Real-Time Attack Management via Telegram:** Attackers receive immediate notifications when victims submit credentials, making phishing more efficient.
- **Massive Increase in Phishing Domains:** Netcraft reports 100,000+ Darcula-linked domains, signaling rapid adoption in cybercriminal communities.

GUIDANCE

Strategic Intelligence

- **Threat Evolution:** Darcula's ability to clone any website and generate phishing kits automatically highlights the growing sophistication of phishing-as-a-service.
- **Cloud Security Concerns:** The increasing abuse of RCS and iMessage demonstrates the need for enhanced detection and filtering mechanisms for modern messaging platforms.
- **Mitigating Phishing Threats:** Organizations must improve phishing prevention, including advanced email filtering and user awareness programs.

Operational Intelligence

- **Attack Vectors**
  - **Initial Access:** Threat actors use Darcula's platform to conduct phishing attacks targeting users via RCS and iMessage.
  - **Credential Harvesting:** Victims are tricked into entering login details, which are then collected and sold or used for further attacks.
  - **Financial Fraud & Monetization:** Stolen credit card details are converted into digital wallet images for in-person fraudulent transactions.
- **Detection & Response Challenges**

RETURN

  - **Credential-Based Attacks:** Traditional defenses struggle to detect phishing attempts that appear identical to legitimate brand websites.
  - **Encrypted Messaging Exploitation:** RCS/iMessage phishing bypasses traditional SMS-based detection tools, requiring new monitoring strategies.
  - **Rapid Deployment & Evolution:** Darcula's easy-to-use interface allows non-technical criminals to quickly launch new campaigns, increasing phishing volume.

- **Security Enhancements for Organizations**
  - **Identity Protection:** Enforce multi-factor authentication (MFA) and monitor login activity for anomalies.
  - **Early Anomaly Detection:** Track new phishing domains and monitor for unusual brand impersonation attempts.
  - **Secure Payment and Account Systems:**
    - Implement real-time fraud detection for high-risk transactions from mobile wallets and burner devices.
    - Enforce device trust policies to prevent compromised accounts from executing unauthorized financial transactions.
  - **Enhance Customer Authentication and Awareness:**
    - Implement phishing-resistant MFA (e.g., FIDO2/WebAuthn) instead of SMS or email OTPs.
    - Educate customers on verifying website URLs before entering sensitive information.
    - Promote official communication channels and discourage clicking on links in unsolicited messages.
  - **Strengthen Employee Training and Awareness:**
    - Conduct regular security awareness training focusing on emerging phishing tactics like RCS/iMessage phishing.
    - Simulate real-world phishing attacks targeting employees to test their ability to detect threats.
    - Provide clear reporting mechanisms for employees to flag suspicious messages and potential phishing attempts.
    - Reinforce the use of corporate-approved password managers to prevent password reuse across personal and professional accounts.
    - Train employees on identifying impersonation attempts, particularly those that exploit business email compromise (BEC) tactics.

Tactical Intelligence

- **Mitigation Strategies**
  - **Restrict Administrative Access:** Limit privileged accounts and enforce just-in-time (JIT) access policies.
  - **Behavioral-Based Endpoint Monitoring:** Use EDR/XDR solutions to detect unusual login behavior and credential theft attempts.
  - **Brand Protection Services:** Engage cybersecurity firms to monitor and take down phishing sites impersonating your organization.

- **Preventive Measures**
  - **Monitor for Brand Impersonation:**
    - Continuously scan for newly registered domains that mimic your organization.
    - Leverage domain takedown services to remove fraudulent websites.
    - Use threat intelligence feeds to detect when your brand is targeted.

RETURN

THREAT HUNTING HYPOTHESES

Phishing via RCS/iMessage to Bypass Security Filters

Hypothesis: Attackers are leveraging Darcula V3's ability to conduct phishing campaigns via RCS and iMessage, bypassing traditional email security measures.

Investigation Approach:

- **Log Analysis:** Review employee and customer reports for phishing attempts via mobile messaging services.
- **Message Content Inspection:** Analyze inbound messages for embedded phishing URLs leading to cloned websites.
- **Behavioral Monitoring:** Track unusual login attempts following mobile-based phishing reports.

Credential Harvesting via Telegram Bot Integration

Hypothesis: Attackers are automating phishing campaigns using Telegram bots to manage stolen credentials and victim tracking.

Investigation Approach:

- **Dark Web & Telegram Monitoring:** Track cybercrime forums and Telegram channels for mentions of Darcula-related phishing services.
- **Domain Traffic Analysis:** Identify bot-generated phishing sites based on sudden spikes in inbound connections.
- **Automated Script Detection:** Analyze bot interaction patterns with phishing site admin panels.

Session Hijacking for Persistent Access

Hypothesis: Threat actors are using stolen session cookies from Darcula phishing campaigns to maintain access without reauthentication.

Investigation Approach:

- **Session Token Analysis:** Monitor for reused or hijacked session cookies in enterprise authentication logs.
- **Unusual Geographic Access:** Detect instances of the same session being used from different geographic regions within a short time frame.
- **Endpoint Security Logs:** Investigate for malware or infostealers that extract browser session data.

RETURN

Exploitation of MFA Fatigue in Phishing Attacks

Hypothesis: Attackers are using repeated MFA push notifications to trick users into approving fraudulent authentication requests.

Investigation Approach:

- **Authentication Log Review:** Identify multiple consecutive MFA requests within a short period.
- **Employee Reporting Trends:** Correlate user reports of unexpected MFA prompts with potential phishing attempts.
- **Anomaly Detection:** Implement machine learning to flag repeated MFA challenges from suspicious IP addresses.

Sources

- **NetCraft:** Darcula V3 Phishing Kits Targeting Any Brand
- **Dark Reading:** Darcula Phishing Service Can Now Auto-Generate Phishing Kits
- **BleepingComputer:** New Darcula Phishing Service Targets iPhone Users via iMessage
- **CyberNews:** Dracula DIY Malware Simplifies Phishing

CAN YOU HELP ME FIX IT?

OVERVIEW & IMPACT

A sophisticated phishing campaign using the ClickFix technique has emerged, leveraging Microsoft SharePoint to deploy the Havoc C2 framework. The attack chain starts with a phishing email containing an HTML attachment that, when opened, displays a fake OneDrive connection error. Victims are then tricked into copying and running a PowerShell command, initiating a multi-stage malware delivery process. The attackers use Microsoft Graph API to obfuscate C2 communications, making detection significantly more challenging.

RETURN

Key Impacts:

- **Cloud Service Abuse:** The campaign exploits Microsoft SharePoint and Graph API, allowing malware to blend into legitimate enterprise traffic.
- **Advanced Post-Exploitation:** Havoc provides attackers with capabilities such as privilege escalation, credential theft, and lateral movement.
- **High Evasion Potential:** The use of cloud-based delivery and encrypted C2 channels complicates traditional security monitoring.
- **Targeted Enterprise Attacks:** Organizations using Microsoft 365 and cloud services are at an elevated risk of compromise and data exfiltration.

OBSERVATIONS

- The campaign demonstrates increased reliance on trusted cloud services (Microsoft SharePoint and Graph API) to evade detection.
- The use of the ClickFix method adds a social engineering layer, leveraging user behavior to bypass security controls.
- Havoc Demon, an alternative to Cobalt Strike, provides advanced post-exploitation capabilities, including token manipulation, privilege escalation, and lateral movement.
- Threat actors are targeting enterprises with cloud-based infrastructures, increasing the risk of undetected data breaches.

GUIDANCE

Strategic Intelligence

- **Threat Evolution:** The integration of Havoc with Microsoft Graph API highlights an emerging trend where attackers exploit enterprise cloud services for stealthy C2 operations.
- **Cloud Security Concerns:** Increased abuse of SharePoint and OneDrive emphasizes the necessity of enhanced monitoring and anomaly detection within cloud environments.
- **Mitigating Phishing Threats:** Organizations must bolster phishing prevention mechanisms, including enhanced email filtering and user awareness programs.

Operational Intelligence

- **Attack Vectors**
  - **Initial Access:** Affiliates exploit stolen credentials, unpatched vulnerabilities, and phishing attacks to gain entry into networks.
  - **Privilege Escalation:** Attackers use exploits and credential abuse to obtain elevated privileges.
  - **Lateral Movement & Data Exfiltration:** Before encryption, data is exfiltrated to leak sites, strengthening extortion tactics.
- **Detection & Response Challenges**
  - **Credential-Based Attacks:** Traditional signature-based defenses may fail to detect unauthorized but legitimate logins.
  - **ESXi & Linux Focus:** Many endpoint security tools lack visibility into non-Windows environments, making detection harder.
  - **Delayed Ransom Deployment:** Affiliates delay execution post-intrusion to avoid immediate detection, making proactive threat hunting essential.
- **Security Enhancements for Organizations**

RETURN

- **Identity Protection:** Continuous monitoring of privileged accounts and enforcing multi-factor authentication (MFA) is critical.
- **Network Segmentation:** Restricting internal network access prevents lateral movement and limits ransomware spread.
- **Early Anomaly Detection:** Monitoring for unusual authentication attempts and data access patterns can detect ransomware actors before deployment.

Tactical Intelligence

- **Mitigation Strategies**
  - **Restrict Administrative Access:** Limit privileged accounts and implement just-in-time (JIT) access policies.
  - **Behavioral-Based Endpoint Monitoring:** Deploy EDR/XDR solutions to detect unusual encryption activity and mass file modifications.
  - **Offline Backups & Immutable Storage:** Ensure backups cannot be modified or encrypted by attackers.
  - **Ransomware-Specific Incident Response Playbooks:** Prepare dedicated ransomware response plans with predefined containment, eradication, and recovery steps.
- **Preventive Measures**
  - **Patch & Vulnerability Management:** Regularly apply security updates to Windows, Linux, and ESXi environments.
  - **Tor & Dark Web Monitoring:** Track Lynx-related leaks and affiliate recruitment posts to identify potential upcoming attacks.
  - **Security Awareness Training:** Conduct phishing simulation exercises to reduce the risk of credential theft-based intrusions.
  - **`Threat Intelligence Integration:** Leverage real-time cyber threat feeds to proactively block Lynx-associated indicators of compromise (IoCs).

THREAT HUNTING HYPOTHESES

ClickFix Exploitation of Microsoft SharePoint for Malware Delivery

Hypothesis: Threat actors are leveraging Microsoft SharePoint to distribute malware payloads via ClickFix phishing campaigns.

Investigation Approach:

- **Log Analysis:** Review SharePoint access logs for unauthorized file uploads containing scripts or executable payloads.
- **User Behavior Monitoring:** Identify abnormal user actions, such as unexpected file downloads and script executions.
- **Threat Intelligence Correlation:** Cross-reference suspicious activity with known Havoc C2 indicators.

Abuse of Microsoft Graph API for Covert C2 Communications

Hypothesis: Threat actors are embedding malicious traffic within Microsoft Graph API to evade detection.

Investigation Approach:

- **API Traffic Analysis:** Monitor for unusual API calls that deviate from normal enterprise usage patterns.
- **Network Traffic Inspection:** Identify outbound traffic interacting with Microsoft cloud services in an abnormal manner.
- **Behavior-Based Alerting:** Deploy analytics-driven detection rules to flag anomalous Graph API activity.

PowerShell Execution Leading to Havoc Deployment

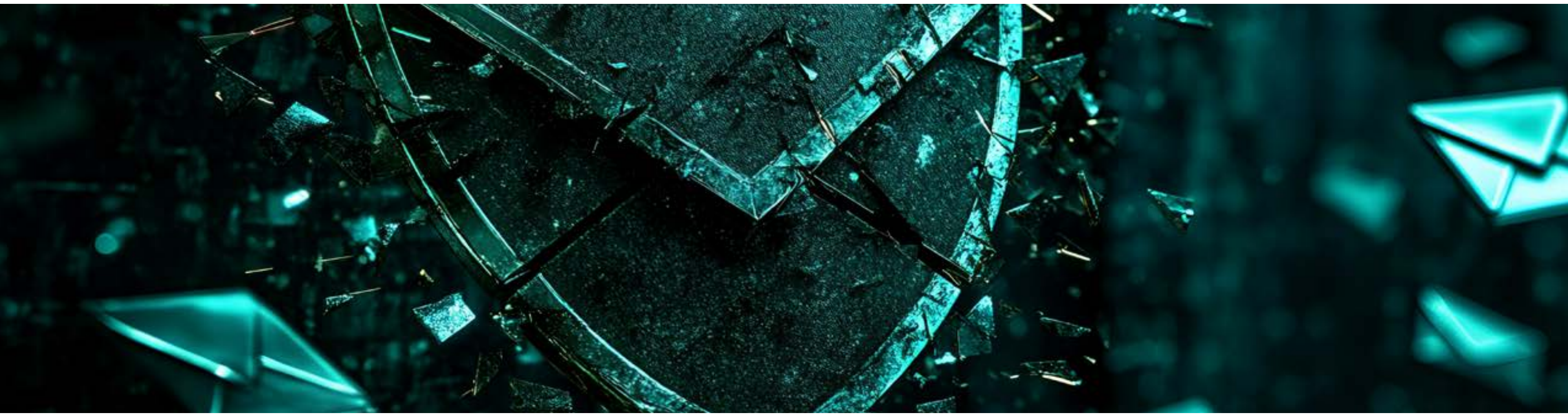
Hypothesis: Threat actors are using PowerShell scripts to download and execute the Havoc C2 framework.

Investigation Approach:

- **Process Execution Monitoring:** Detect PowerShell scripts executing commands to fetch content from SharePoint URLs.
- **Endpoint Forensics:** Investigate signs of persistence mechanisms related to Havoc Demon.
- **File Integrity Analysis:** Track unauthorized modifications or execution of Python binaries from non-standard directories.

Sources

- **Dark Reading:** Phishers Wreak Havoc Disguising Attack Inside SharePoint
- **BleepingComputer:** New ClickFix Attack Deploys Havoc C2 via Microsoft SharePoint
- **TechRadar:** Microsoft SharePoint Hijacked to Spread Havoc Malware
- **The Hacker News:** Hackers Use ClickFix Trick to Deploy Havoc Malware



CONVERGE
TECHNOLOGY SOLUTIONS

Contact the Converge Threat Intel Group at cybersecurity@convergetp.com

convergetp.com/cybersecurity