Apollo THREAT INTELLIGENCE

TLP:GREEN

THE RISE OF ROYAL RANSOMWARE:

THREATS TO MUNICIPALITIES & EMERGENCY SERVICES

Apollo Information Systems Corp.

TLP:GREEN

Traffic Light Protocol:	**GREEN:** *Recipients may share information with peers and partner organizations within their sector or community, but not via publicly accessible channels.*
Importance:	**Critical**
Intelligence Type:	**Threat Actor - Cyber Criminal**
Issue Date:	9 May 2023

The Rise of Royal Ransomware:

Threats to Municipalities and Emergency Services

Summary

The threat of Royal ransomware is escalating, presenting significant risks to municipalities and emergency services as cybercriminals refine their tactics to maximize the impact of their attacks. Backed by the former notorious Conti ransomware gang, the Royal ransomware group poses a substantial danger to critical infrastructure sectors worldwide, especially those involved in handling sensitive data and ensuring public safety.

Municipalities face unique challenges due to limited cybersecurity resources and budget constraints, making it difficult to keep up with the ever-evolving cyber threat landscape. Outdated technology and legacy systems further compound the risks, making these organizations attractive targets for cybercriminals. Ransomware attacks on cities have severe consequences, as extended system downtime is not an option for critical services. The pressure to pay ransoms intensifies with the potential loss of revenue and public trust as cybercriminals exploit psychological tactics to create a false sense of urgency.

Royal ransomware has impacted 29 US local governments, severely affecting emergency services.

To mitigate these risks, state and local governments must prioritize cybersecurity by raising employee awareness, providing comprehensive training, investing in robust information security programs, and collaborating with organizations that adhere to good cyber hygiene practices. Emergency services, such as 911 systems, police departments, fire departments, and water utilities, are particularly vulnerable to ransomware attacks, which pose a risk to public safety and impact citizens.

The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) have issued joint warnings about the increasing number of Royal ransomware attacks targeting critical infrastructure sectors. The Royal ransomware group utilizes advanced infection vectors and tactics, making them formidable adversaries. This threat brief focuses on the impact of these attacks on municipalities and emergency services, providing insights into the group's methods and suggesting mitigation strategies to counter their activities.

Addressing these challenges requires an enhanced cybersecurity posture. Municipalities and emergency services must implement comprehensive security measures, enhance employee awareness, and adopt modern technology to combat cybercriminals and protect their communities.

Adopting a proactive cybersecurity approach is crucial, relying on actionable intelligence and proactive defense measures to prevent attacks before they occur.

One valuable aspect of proactive defense is leveraging darknet threat intelligence. The darknet, a hidden part of the internet used for illicit activities, provides crucial insights into emerging cyber threats, including advanced persistent threats, zero-day exploits, insider threats, and ransomware distribution. Investing in darknet threat intelligence allows organizations to proactively identify and mitigate threats, enhance overall security posture, and improve regulatory compliance and risk management.

Darknet marketplaces serve as a haven for cybercriminals, with brokers selling access lists for U.S. cities and counties. Disrupting cybercriminals' crime model involves refusing to pay ransoms and making their activities cost prohibitive. Leveraging directed intelligence and adopting a preemptive cybersecurity approach is essential to protect public safety, prevent attacks, and stay one step ahead of adversaries.

Emergency services, including 911 systems, police departments, fire departments, and water utilities, remain prime targets for ransomware attacks due to their critical nature. Disruptions to these services can have dire consequences for public safety. By acting on early intelligence, addressing vulnerabilities, implementing common-sense security measures like multifactor authentication (MFA), fostering employee awareness, and utilizing advanced technologies are crucial to mitigate the risks posed by cybercriminals.

The rising threat of Royal ransomware and others demands a proactive response from municipalities and emergency services. By leveraging intelligence, adopting robust cybersecurity measures, enhancing employee awareness, and investing in modern technology, these organizations can bolster their defenses and protect their communities. Close collaboration with the FBI, CISA, and other relevant authorities is vital for sharing intelligence, staying informed about evolving threats, and implementing effective mitigation strategies to counter the activities of the Royal ransomware group.

It is recommended that organizations perform the following actions immediately:

- Prioritize the remediation of known vulnerabilities in your environment.
- Train users in recognizing and reporting phishing attempts.
- Implement and enforce Multi-Factor Authentication (MFA).

Key Points

Infection Vectors and Targeted Industries

- Royal ransomware targets critical infrastructure sectors, affecting emergency services, transportation, manufacturing, technology, education, healthcare, and government organizations.
- The group has impacted **29** US local governments, severely affecting emergency services.

Attack Techniques

- Royal actors utilize callback phishing campaigns, web vulnerability exploitation, and abuse of Google Ads to gain initial access.
- They employ post-exploitation frameworks, such as Cobalt Strike, PowerSploit, MegaCMD, and SharpExfiltrate, for persistent access and data exfiltration.
- The group uses a unique partial encryption method to evade detection and engages in double extortion tactics, threatening to release encrypted data unless the ransom is paid.

Recent Incident

- A major U.S. city has been significantly impacted by a Royal ransomware attack, disrupting police operations and city services.
- Local governments are appealing targets due to valuable data, resource constraints, and the necessity to maintain critical services.

Mitigation Strategies

- Prioritize the remediation of known vulnerabilities.
- Train users in recognizing and reporting phishing attempts.
- Implement and enforce multifactor authentication (MFA).
- Educate employees about cyber threats, allocate resources to information security programs, and deploy advanced security technologies.

Conti Rebranding

Conti was a Russian ransomware operation that began in 2020 as a successor to Ryuk ransomware. The group evolved into a cybercrime syndicate, taking over the development of malware operations like TrickBot and BazarBackdoor. Following their public support for Russia's invasion of Ukraine, internal chats and the Conti ransomware encryptor source code were leaked online. In May of 2022, the gang divided into smaller cells, with members infiltrating and taking over other ransomware operations such as HelloKitty, AvosLocker, Hive, BlackCat, and BlackByte, which allowed them to stay active and evade law enforcement. One of the resulting groups is Royal ransomware, which quickly became a significant and evolving threat to organizations worldwide. This technical brief discusses the activities and mitigation strategies for dealing with the Royal ransomware group. Royal ransomware, a rebranded version of Zeon ransomware, is linked to Conti Team One, which was involved in Conti ransomware distribution. Conti was known for their Ransomware-as-a-Service (RaaS) attack model and extremely aggressive tactics. Attacks included Ireland and Costa Rica.

Sample Ransom Note:
"If you are reading this, it means that your system were hit by Royal… Most likely what happened was that you decided to save some money on your securi(ty)… Royal offers you a unique deal. For a modest royalty (got it; got it?) for our…covering you from reputational, legal, financial, regulatory, and insurance risk…your files will be decrypted, your data restored and kept confi(dential)."

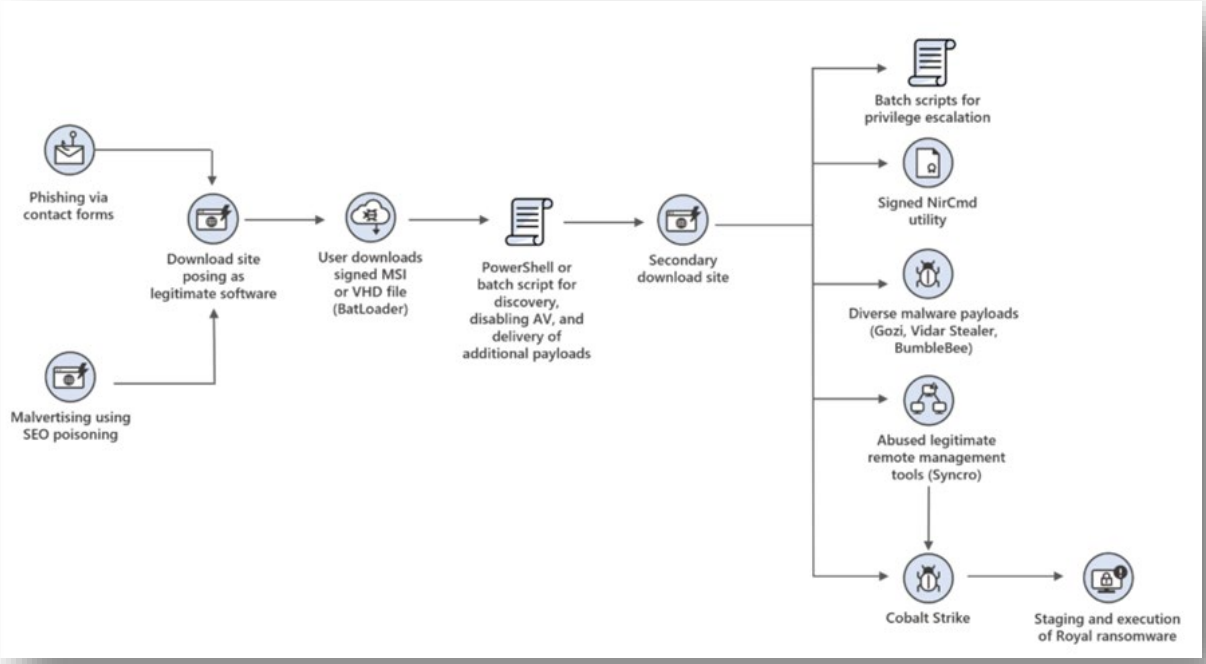

Image 1: Infection Chain, Diagram Source: Microsoft Intelligence

Infection Vectors & Targeted Industries

- The Royal ransomware group has targeted critical infrastructure sectors globally since September 2022.
- Industries affected include emergency services, transportation, manufacturing, technology, education, healthcare, and government.
- Specifically targeted sectors are Manufacturing, Communications, Healthcare and Public Healthcare (HPH), and Education.
- Phishing emails are the primary infection vector, accounting for 66.7% of successful compromises.

Attack Techniques

- Royal actors disable antivirus software upon gaining access to victim networks.
- Ransomware is deployed, encrypting systems, and preventing intervention.
- Ransom demands range from $1 million to $11 million in Bitcoin.
- The group utilizes traditional and novel techniques, including callback phishing, intermittent encryption, and exploitation of web vulnerabilities.
- The group quickly adapted and developed Linux-based variants to expand their target range.
- Over 100 organizations have been compromised, with at least 16 experiencing data theft.

Initial Access Methods

- Callback phishing campaigns impersonate food delivery or software providers, tricking victims into installing remote access software.
- Exploiting web vulnerabilities is an initial access method, indicating higher sophistication.
- Initial access through the abuse of Google Ads is one method to deliver malware, such as BatLoader.

Tools & Malware

Security teams should take note of and observe the presence of the following malware and tools typically used in Royal ransomware attacks:

Tools

- PsExec
- NetScan
- AdFind
- CobaltStrike
- PCHunter
- Process Hacker
- GMER
- PowerTool
- RDPEnable
- RClone
- Connectwise
- Splashtop
- Atera
- Syncro
- Advanced Port Scanner

Malware

- Batloader
- QakBot
- IcedID
- Gozi
- Vidar

Tactics, Techniques, and Procedures (TTPs)

Enterprise T1486 - Data Encrypted for Impact

- Royal uses a multi-threaded encryption process to partially encrypt targeted files with the OpenSSL library and the AES256 algorithm.[2][3][4]

Enterprise T1083 - File and Directory Discovery

- Royal can identify specific files and directories to exclude from the encryption process.[2][3][4]

Enterprise T1490 - Inhibit System Recovery

- Royal can delete shadow copy backups with vssadmin.exe using the command delete shadows /all /quiet.[2][3][5]

Enterprise T1106 - Native API

- Royal can use multiple APIs for discovery, communication, and execution.[2]

Enterprise T1046 - Network Service Discovery

- Royal can scan the network interfaces of targeted systems.[2]

Enterprise T1135 - Network Share Discovery

- Royal can enumerate the shared resources of a given IP addresses using the API call NetShareEnum.[2]

Enterprise T1095 - Non-Application Layer Protocol

- Royal establishes a TCP (Transmission Control Protocol) socket for C2 communication using the API WSASocketW.[2]

Enterprise T1566 - Phishing

- Royal has been spread using phishing campaigns including "call back phishing" where victims are lured into calling a number provided through email.[2][3][5]

Enterprise T1057 - Process Discovery

- Royal can use GetCurrentProcess to enumerate processes.[2]

Enterprise T1021.002 - Remote Services: SMB/Windows Admin Shares

- Royal can use SMB (Server Message Block) to connect to move laterally.[2]

Enterprise T1489 - Service Stop

- Royal can use RmShutDown to kill applications and services using the resources that are targeted for encryption.[2]

Enterprise T1082 - System Information Discovery

- Royal can use GetNativeSystemInfo and GetLogicalDrives to enumerate system processors and logical drives.[2][4]

Enterprise T1016 - System Network Configuration Discovery

- Royal can enumerate IP addresses using GetIpAddrTable.[2]

Post-Exploitation & Exfiltration

- The group utilizes post-exploitation frameworks like Cobalt Strike and tools such as PowerSploit, MegaCMD, and SharpExfiltrate.
- The group maintains persistent access through Cobalt Strike.

Encryption & Extortion Tactics

- Royal ransomware uses a unique partial encryption approach, allowing threat actors to selectively encrypt a specific percentage of data in a file.
- Larger files have lower encryption percentages, aiding in evading detection.
- In addition to encryption, the group uses double extortion tactics, threatening to release encrypted data unless the ransom is paid.

Mitigation Recommendations

Adopting these recommendations can significantly reduce the probability and impact of ransomware incidents. Organizations must remain vigilant and proactive in addressing the ever-evolving threat landscape presented by groups like the Royal ransomware group.

To effectively counter the risks associated with Royal ransomware, consider implementing the following:

User Education and Access Control

- Educate employees on ransomware threats, prevention techniques, phishing tactics, and safe browsing habits.
- Enforce regular password changes and encourage strong, unique passwords following National Institute of Standards and Technology (NIST) best practices.
- Implement Multi-Factor Authentication (MFA) for all accounts and users.
- Review and strengthen access control policies, granting access on a "need to know" basis.
- Immediately force password changes for administrator accounts and revoke password-change privileges for executive administrative assistants.

Network and System Security

- Manage your assets: Maintain an up-to-date inventory of your organization's IT assets, including logical (e.g., data, software) and physical (e.g., hardware) components.
- Use multi-layer malware protection leveraging threat intelligence, machine learning, anti-ransomware, next-gen antivirus (NGAV), and Variant Payload Prevention capabilities.
- Maintain up-to-date antivirus software and regularly patch software, web vulnerabilities, VPNs, and DMZ access points.
- Implement network segmentation, access controls, and micro-segmentation to limit lateral movement within the network during a breach.
- Deploy intrusion detection and prevention systems for early warnings and blocking malicious activities.
- Review and update firewall rules to restrict inbound and outbound traffic and establish firewalls between VLANs.
- Disable command line scripting.

Backup and Incident Response

- Regularly back up data and store backups offline; consider using backup technology that provides immutable backups.
- Develop and test an incident response plan for isolating infected systems, investigating breaches, and restoring operations promptly.

Monitoring and Assessment

- Be vigilant about Callback Phishing scams and review your environment for non-standard remote desktop software like AnyDesk, LogMeIn, and Atera.
- Conduct vulnerability assessments and ensure the timely patching of all vulnerabilities, especially in your DMZ.

- Continuously monitor and scan file systems for any signs of malicious activity. d. Hire a reputable, outside firm to conduct periodic tabletops, compromise assessments, and vulnerability scans.

External Resources

- Partner with your local FBI field office to get ahead of cyber threats: https://www.fbi.gov/investigate/cyber
- Visit CISA for more information on ransomware prevention: https://www.cisa.gov/stopransomware
- Hire a reputable, outside firm to conduct periodic tabletops, compromise assessments, and vulnerability scans.
- CISA recommends that organizations consider the following external resources, provided here:

Response & Recovery Recommendations

During a Royal ransomware attack, it is critical to act quickly and methodically. We have outlined essential steps to follow.

Detection and Analysis

- Identify impacted systems, isolate them, and disconnect them from the network.
- Perform in-depth log analysis and traffic monitoring to identify malicious activities.
- Prioritize critical assets for restoration based on a predefined list.
- Collaborate with internal and external stakeholders to gather relevant information and develop an initial understanding of the incident.

Immediate Response

- Activate the incident response team and initiate communication protocols.
- Inform relevant stakeholders and senior leadership of the incident.
- Isolate affected systems and devices from the network to prevent the further spread of ransomware.

Containment and Eradication

- Create system images and memory captures of affected devices for forensic analysis.
- Collect relevant logs, samples of precursor malware binaries, and associated observables or indicators of compromise.
- Consult with federal law enforcement for potential decryptor tool availability.

Engaging External Support

- Collaborate with external cybersecurity experts to assist in incident response.
- Notify law enforcement agencies and share relevant information.

Recovery and Restoration

- Utilize available tools to decrypt and restore data.
- Avoid paying the ransom to discourage future attacks and prevent potential legal implications due to sanctions.
- Allocate resources for rebuilding systems using clean hardware and software.
- Implement virtualization when rebuilding systems to improve resilience.

Security Measures for Sensitive Assets

- Strengthen security measures for sensitive assets, including DMZ and other critical systems.
- Apply network segmentation, micro-segmentation, and access controls to limit lateral movement during a breach.

Post-Incident Actions

- Review and update security measures based on lessons learned.
- Conduct a thorough post-incident analysis to identify areas for improvement.

Ongoing Prevention and Monitoring

- Establish and implement a proactive ransomware prevention plan.
- Continuously monitor systems and networks, particularly DMZ and other sensitive assets, for potential threats and vulnerabilities.

References & Resources

1. MSTIC. (2022, November 17). DEV-0569 finds new ways to deliver Royal ransomware, various payloads. Retrieved March 30, 2023.
2. Cybereason Global SOC and Cybereason Security Research Teams. (2022, December 14). Royal Rumble: Analysis of Royal Ransomware. Retrieved March 30, 2023.
3. Iacono, L. and Green, S. (2023, February 13). Royal Ransomware Deep Dive. Retrieved March 30, 2023.
4. Morales, N. et al. (2023, February 20). Royal Ransomware Expands Attacks by Targeting Linux ESXi Servers. Retrieved March 30, 2023.
5. CISA. (2023, March 2). #StopRansomware: Royal Ransomware, Retrieved March 30, 2023
6. CISA Cybersecurity Advisories. (n.d.). Retrieved from https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a
7. IC3. (2021, May 21). Retrieved from https://www.ic3.gov/Media/News/2021/210521.pdf
8. American Public Power Association. (n.d.). Public Power Cyber Incident Response Playbook. Retrieved from https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf
9. Center for Internet Security. (n.d.). Security Primer: Ransomware. Retrieved from https://www.cisecurity.org/white-papers/security-primer-ransomware/
10. United States Secret Service., Preparing for a Cyber Incident: A Guide to Ransomware. Retrieved from https://www.secretservice.gov/sites/default/files/reports/2021-11/Preparing%20for%20a%20Cyber%20Incident%20-%20A%20Guide%20to%20Ransomware%20v%201.1.pdf

USE CASE: Anatomy of an Attack

Below is a synopsis of a recent ransomware attack by Royal.

Reconnaissance

- Constant scanning highlights municipalities when errors or changes in business logic create the potential for access.
- Municipalities are choice targets to identify.

Discovery and Sale

- Post discovery, cybercriminals quietly gain access and insert a means to return.
- This initial access is sold, either as an auction or an offering.

Initial Exploit

- Attackers purchased network access from a broker.
- A renamed version of NetSupport Manager was installed during a previous incident.
- The original phishing email could not be found due to log rollover.
- The actors used Netscan, ADFind, and batch scripts for reconnaissance.
- They also used "net user" and "net localgroup" commands for environment mapping.

Toolkit Deployment

- Legitimate remote access tools, such as Splashtop, Atera Agent, and AnyDesk, were used for command and control.
- Cobalt Strike was deployed for additional control.

Antivirus EDR Disabled

- Microsoft Defender was disabled with PowerShell commands.
- PowerTool64.exe and GMER were used to remove EDR software.

Escalation

- PowerSploit was used to identify machines with local administrator privileges.

Lateral Movement

- Remote Desktop Protocol (RDP) was used for navigation, followed by remote access tool installation and antivirus/EDR disabling on new devices.

Mission Execution

- SharpExfiltrate and Megacmd.exe were used to exfiltrate sensitive information.
- Ransomware binary execution occurred via a batch script.

Recommendations

- Monitor PowerShell execution and log encoded script execution.
- Audit user, administrator, and service accounts to enforce the principle of least privilege.
- Implement multifactor authentication to restrict access and prevent lateral movement.
- Review backup strategies, ensuring multiple isolated backups.
- Review and whitelist remote access tools; limit their usage within the network.

Indicators of Compromise (IoC)

- Various files, hashes, and external IP addresses were observed during the incident. Please refer to the updated IoC (Indicators of Compromise) list for details.
- Current IoCs (Indicators of Compromise) can be found here. https://www.cisa.gov/sites/default/files/2023-03/aa23-061a.stix__0.xml

Snapshot of Ransomware Attacks on City Governments and Departments

This list does not encompass all incidents but provides insight into recent ransomware attacks. As of the date of this brief, a significant U.S. city is grappling with service disruptions resulting from a Royal ransomware attack. Affected services include 911 capabilities and other emergency services provided by police and fire departments.

We have observed at least a dozen access sales for cities on the darknet. Predictive analysis models suggest that ransomware attacks may target these cities within 60-90 days. Our ongoing efforts include continuous intelligence gathering and responsible disclosure to address this evolving threat.

2023

- January 3, 2023: Swansea Public Schools - Swansea, Massachusetts, USA
- January 30, 2023: Tucson Unified School District - Tucson, Arizona, USA
- February 3, 2023: Hidalgo County Adult Probation Center - Edinburg, Texas, USA
- February 5, 2023: City of Oakland - Oakland, California, USA
- February 17, 2023: United States Marshals Service (USMS) - Arlington, Virginia, USA
- February 20, 2023: Washington County Sheriff's Office (WCSO) - Chipley, Florida, USA
- April 22, 2023: North Kingstown, Rhode Island, USA
- April 27, 2023: Spartanburg County - Spartanburg, South Carolina, USA
- May 1, 2023: A major U.S. city Police Department - USA (Royal Ransomware)

$70 billion in downtime costs

Excluding the remainder of 2022 and 2023, ransomware attack statistics from 2018 to October 2022 are as follows: According to data from Comparitech, during this period, 330 individual ransomware attacks targeted U.S. government organizations. These attacks potentially affected over 230 million people and resulted in an estimated $70 billion in downtime costs alone.

- https://www.comparitech.com/blog/information-security/government-ransomware-attacks/

About Apollo

The cyber threat landscape is rapidly evolving, and organizations must adopt innovative defense strategies and best practices to survive and thrive. **Cybercrime costs are projected to exceed 3.5% of global GDP by 2030,** necessitating a forward-thinking and adaptable approach to cybersecurity. By investing wisely, prioritizing risk reduction aligned with business objectives, and actively monitoring risks, organizations can successfully navigate this complex landscape.

Apollo Information Systems Corp. (Apollo) is distinguished by our proactive and preemptive approach to cybersecurity, leveraging directed advanced intelligence to prevent attacks before they happen. Our methodology incorporates multiple forms of intelligence, including HUMINT (human intelligence), to support cybercrime disruption, enhance public safety, and protect national security.

As a trusted security partner serving high-stakes organizations and businesses across various industries and government entities, Apollo's extensive expertise, commitment to innovation, and strategic collaborations empower clients to achieve operational excellence. We prioritize safeguarding what matters most to your organization, providing practical, cost-efficient solutions that maximize the value of every dollar invested.

Our comprehensive service portfolio is tailored to the specific needs of each client and includes Deep Insight Threat Intelligence Capability, Managed Services, Election Security, and more. Apollo's services support SLED, FED, and Enterprise.

We work closely with clients to understand their unique requirements and deliver specialized offerings through world-class Chief Information Security Officers (CISOs), Security Architects and Engineers, Chief Information Officers (CIOs), and professionals with Secret and Top-Secret clearances. We are committed to meeting the most stringent industry standards, as demonstrated by our Systems and Organization Controls 2 (SOC2) Certified Security Operations Center and CJIS compliance.

At Apollo, our unwavering commitment to customer success and tangible value delivery is backed by a practitioner-led approach and a team of experienced IT and cybersecurity specialists, ensuring clients receive top-tier expertise and achieve meaningful results. By combining industry best practices with our advanced intelligence-driven approach, Apollo empowers organizations to confidently navigate an ever-evolving landscape of threats and uncertainties, effectively mitigating potential risks and securing what matters most.

Apollo's services are available on GSA Advantage through Cyberdefenses.

Contact Us
Phone: (408) 399-5110
https://www.apollo-is.com

Experiencing a Breach? CALL (833) 292-3701

TLP:GREEN

FLIPPING THE SCRIPT

CREATING A SECURE WORLD IS NOT JUST A PROMISE IT'S OUR PURPOSE

Apollo THREAT INTELLIGENCE

TLP:GREEN