KROLL

THE MONITOR

VOLUME 5

VPN Vulnerabilities Tied to Rising Data Exposure, Ransomware

Kroll reviewed a wide variety of incident response cases in recent weeks that involved some sort of remote access compromise. With record numbers of employees now working from home, accidental and malicious data exposure incidents are on the rise, many of which are due to vulnerabilities associated with virtual private network (VPN) or remote desktop protocol (RDP) connections.

While VPNs are traditionally more secure than RDP solutions, several VPN providers released significant software patches in the past year, a fact that cybercriminals were quick to seize on. Organizations that haven't updated their VPN software are now prime targets for ransomware operators and other malicious actors. In a recent Cybersecurity Advisory, the National Security Agency (NSA) urged organizations to check VPN products for upgrades. The advisory warned, "Upgrade your VPN products to the latest vendor-released versions to protect your networks from these attacks. The known vulnerabilities include Pulse Secure™, Palo Alto GlobalProtect™ and Fortinet FortiGate™ VPN products."

Pulse Secure VPNs are particularly vulnerable due to the critical CVE-2019-11510 alert issued by the company last year for a flaw that allows for remote authentication to a VPN appliance. Pulse Secure's advisory stated vulnerabilities could "allow an unauthenticated user to perform a remote arbitrary file access on the Personal Communication Service (PCS) gateway... and allow an authenticated administrator to perform remote code execution...", both of which the advisory further added, "pose significant risk to your deployment." This advisory was updated in 2020 to reflect new exploitation information and recommendations. Given the fact that there is no workaround, the Cybersecurity and Infrastructure Security Agency (CISA) recommends applying patches provided by the vendor and performing all necessary system updates.

How Do Threat Actors Exploit Vulnerable VPNs?

Actors are mainly identifying potential corporate targets by scanning the internet and then gaining access to user accounts via known exploits. Skip to the "Exploit in Action" section of this newsletter to see a video demonstration.In the past, threat actors most often compromised VPNs through "session hijacking," after getting their hands on a valid session ID through means such as brute-force attacks or reverse engineering.

Thomas Brittain, Associate Managing Director at Kroll, said that has dramatically changed. He commented, "We've been seeing engagements where actors are getting access without session hijacking and that's due to CVE-2019-115110's pre-authentication vulnerability that allows unimpeded access. Essentially, actors can query the vulnerable VPN to pull a unique ID for an account, then leverage web browser development tools to manually set a value to the ID, and that allows them unauthenticated access to the VPN administrator console." From there, it's generally short work for actors with system access to remotely connect to internal systems. Once on your internal network, they download and execute programs and commands to conduct reconnaissance and harvest passwords enabling them to move laterally in the network and, in many cases, prepare to deploy ransomware.

See a CVE-2019-115110 Exploit in Action

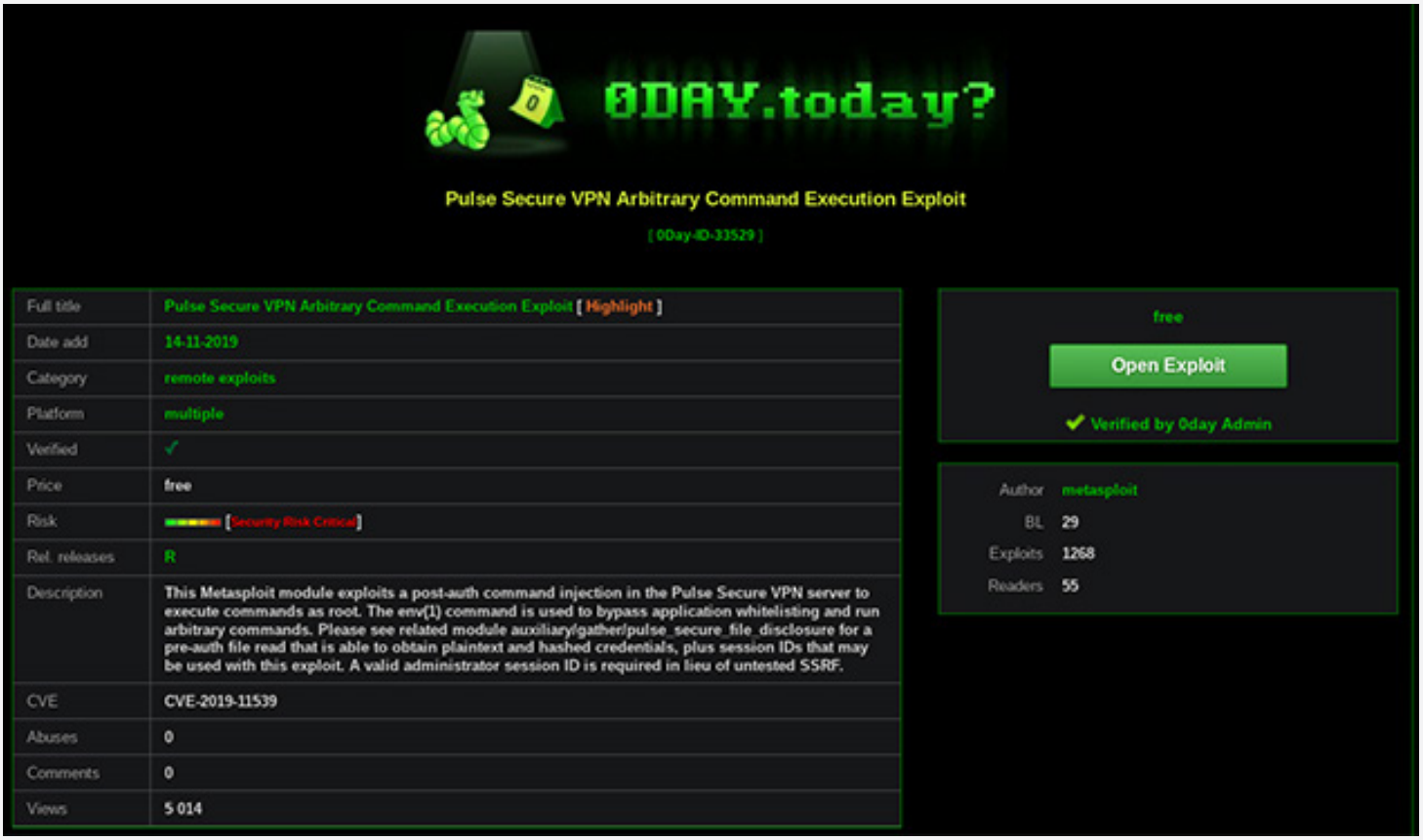
The video below demonstrates how the vulnerability can be exploited in an unpatched system. Actors remotely scana system to extract an admin session ID and then bypass the admin login screen by loading the session ID to the browser console, which gives them unauthenticated access to all admin functions. In this example, actors force Windows's calculator app to load after a VPN user connects to the network, but a real attack would execute more damaging scripts.

To view the video, visit kroll.com/monitor-issue-13

In addition to financially motivated actors targeting vulnerable VPNs, advanced persistent threat (APT) groups have also been capitalizing on unsecured VPN infrastructure. Microsoft threat intelligence teams have observed multiple nation-state and cybercrime actors targeting unpatched VPN systems for many months. In October 2019, both the National Security Agency (NSA) and National Cyber Security Centre (NCSC) put out alerts on these attacks and encouraged enterprises to patch. These actors could leverage exploits to target newly created VPN appliances to gain access to intellectual property or other sensitive data on company networks.

VPN Exploits on the Dark Web

Often the initial challenge in exploring vulnerabilities is finding a way to exploit them, as it involves careful research and may require a rethink of existing attack vectors. Sophisticated exploit scripts can go for thousands of dollars in dark web markets, and some particularly impactful exploit tools are actually considered military weapons. For CVE-2019-11539, however, effective exploits are available on the dark web for free, as you can see below:



Case Studies

Kroll's recent case studies emphasize the critical need for organizations to know the current status of their VPN infrastructure and apply all patches prior to connecting to the internet.

- Sodinokibi ransomware actors entered a client's system through a vulnerability in Pulse Secure VPN. The actor began deploying the ransomware across all the client's servers and later sent ransom demands, threatening to publish exfiltrated data.
- Actors struck just one to two days after a client added two unpatched VPN appliances to their network. Kroll's investigation found that prior to a ransomware attack, credentials for the client's domain administrator and IT director were compromised. Two new domain admin accounts were created by the actors once they gained access to the network. This example demonstrates the importance of patching vulnerable VPN appliances, as quickly as possible.

Thomas Brittain
Associate Managing Director

Kroll Experts Corner:
Best Practices for Securing VPNs

As organizations contend with remote networking challenges, VPN security is imperative. Thomas Brittain has provided several best practices to help prevent the compromise of VPN appliances, related data exposure and ransomware attacks:

Immediate Mitigation Recommendations

- Update and apply all patches and secure configurations of any VPN or other edge/gateway appliance before placing on your network or connecting to the internet
- Enable multifactor authentication (MFA) or two-factor authentication (2FA) for all user accounts leveraging external access over VPN or RDP services; enforce regular password resets that include a complex password policy
- Reset all local VPN accounts, VPN users, administrators and service account credentials before reconnecting upgraded devices to the internet
- Revoke and create new VPN server keys and certificates
- Review your network accounts to ensure adversaries did not create new accounts

Additional Recommendations

- Minimize or eliminate remote access for administrator accounts through VPN or RDP services. Leverage a user account with limited privileges and once logged in to your internal network, switch user accounts.
- Enable logging on all VPN and/or firewall appliances to track all authentication events (successful, failed and unauthenticated), user activity such as RDP connections, file access/downloads and the volume of data (e.g., Cisco's NetFlow protocol) transmitted and received.
- If possible, send all logs to a Security Information and Event Management (SIEM) system, which can serve as a centralized event and log data collection and analysis point.
- Create a process to review, test and update any edge/internet-connected systems regularly.

Crucial Consideration for the New Normal

Even though some organizations are already planning to return their employees to offices, the move will be gradual; many organizations may prefer to continue remote working indefinitely. VPN configuration remains a crucial step in protecting a remote workforce, and it's imperative that vulnerabilities like CVE-2019-11539 and CVE-2019-115110 are addressed, along with many others, as part of a robust vulnerability management program. For further guidance, contact a Kroll expert at one of our 24x7 cyber incident response hotlines or our Contact Us page.

Telerik Vulnerability (CVE-2019-18935) Creates Surge in Web Compromise and Cryptomining Attacks

In May 2020, Kroll began observing an increase in compromises related to vulnerabilities in Telerik user interface (UI) software, a spinoff of Telerik's web software tools which provides navigation controls. The vulnerability, which is outlined in CVE-2019-18935, involves a .NET deserialization vulnerability in the software that allows for remote code execution.

Kroll observed more than a dozen cases in a short span of time in which attackers targeted the Telerik vulnerability to deploy remote access tools or credential harvesting software and then gain remote access to the client's network. The most often targeted clients observed by Kroll within the sample timeframe were in the healthcare and government sectors (Figure 1).

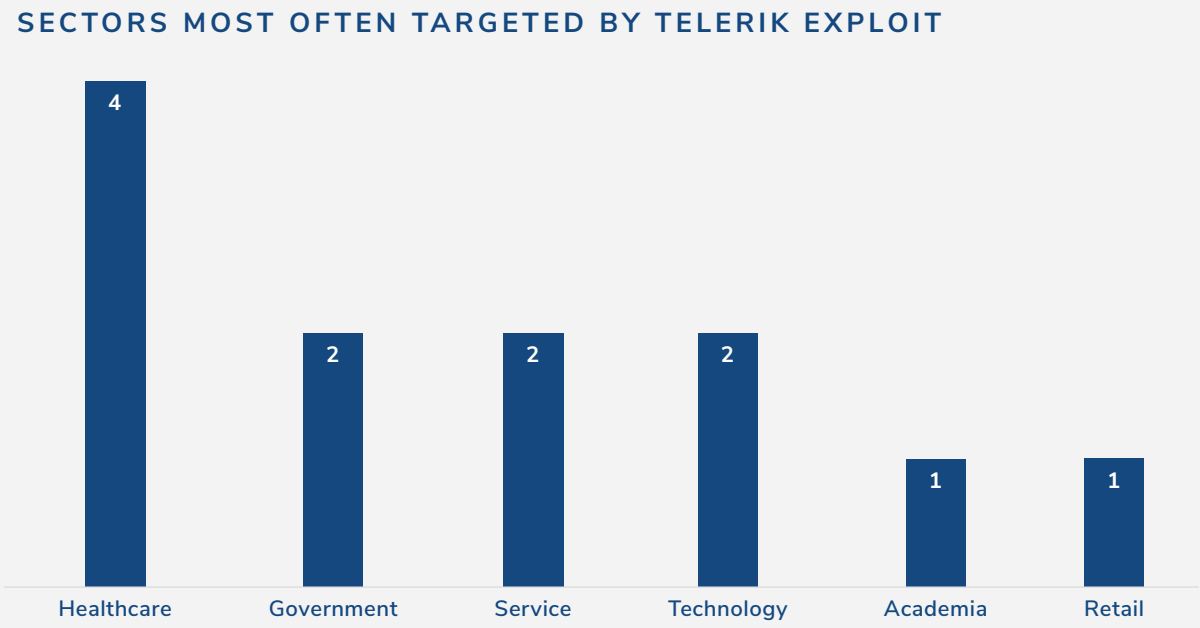


Figure 1 - Sectors Most Often Impacted by Telerik Exploits

How Do Threat Actors Exploit the Telerik Vulnerability?

The deserialization attack enabled by CVE-2019-18935 is different from the previously exposed encryption flaw in CVE-2017-11317, which allowed unrestricted file uploads. In the deserialization attack, rather than submitting the expected Telerik.Web.UI.AsyncUploadConfiguration type with rauPostData, an attacker can submit a file upload POST request specifying the type as a remote code execution gadget instead. This gives attackers the ability to execute software, code or webshells indiscriminately within the webservice.

Kroll was able to pinpoint attacks by examining available forensic evidence and most critically, web server access logs, looking specifically for unique user-agent strings and IP addresses previously flagged by our threat intelligence team. Investigating those strings and activity tied to their interactions with internet facing servers revealed suspiciously uploaded files, ranging from .aspx, .js, to .zip content. Kroll's analysis of identified files revealed a range of capabilities across different impacted systems from code injection and remote access to credential harvesting.

Anthony Knutson, Senior Vice President in Kroll's Cyber Risk practice, provided more details: "Specifically in the webshells, our engineers were able to recreate what the threat actor would see when traversing specific pages and demonstrate how these webshell files could go undetected by requiring the specific user-agent string we mentioned. Without that user-agent string, the page would load as an HTTP 404 error, and the webshell would not activate."Devon Ackerman, Managing Director and Head of North America Incident Response, added: "Like most webshells leveraged by attackers, these shells provided the unauthorized actors with abilities ranging from direct SQL database access, to file read/write capabilities, to operating system-level remote command prompt and PowerShell access."

> Specifically in the webshells, our engineers were able to recreate what the threat actor would see when traversing specific pages and demonstrate how these webshell files could go undetected by requiring the specific user-agent string we mentioned. Without that user-agent string, the page would load as an HTTP 404 error, and the webshell would not activate.

Reported Large-Scale Telerik Vulnerability Exploitation

In early June, Australia suffered a large volume of state-sponsored attacks related to the Telerik UI vulnerability.The government observed advanced persistent threat (APT) scanning for unpatched versions of the Telerik vulnerability and leveraging publicly available exploits to attempt to exploit these systems. "The actor has been identified leveraging a number of initial access vectors, with the most prevalent being the exploitation of public-facing infrastructure — primarily through the use of remote code execution vulnerabilities in unpatched versions of Telerik UI," the report stated.

According to recent reporting by the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC), a group dubbed Blue Mockingbird recently infected thousands of computer systems via the Telerik vulnerability. "The group conducted a cryptocurrency mining campaign by targeting public-facing servers running ASP.NET apps using the Telerik framework. By exploiting CVE-2019-18935, the group was able to install a web shell in the compromised server and then used a privilege escalation tool to gain accesses needed to modify server settings and maintain persistence," the report stated. Devon Ackerman, Managing Director in Kroll's Cyber Risk practice, added, "In Kroll's estimation, for the investigations where actor groups have leveraged the Telerik vulnerability to push in cryptocurrency mining operations, the activity was noisy and burdensome to the impacted systems.In every case that Kroll investigated involving this methodology, the client's IT and security team had already noted the system resource impact tied to the miners—it wasn't stealthy, it wasn't a structured attack, but it was noisy, like a thief stumbling through a victim's home knocking over lamps and cabinets alerting everyone within ear shot of their presence."

In Kroll's estimation, for the investigations where actor groups have leveraged the Telerik vulnerability to push in cryptocurrency mining operations, the activity was noisy and burdensome to the impacted systems.In every case that Kroll investigated involving this methodology, the client's IT and security team had already noted the system resource impact tied to the miners—it wasn't stealthy, it wasn't a structured attack, but it was noisy, like a thief stumbling through a victim's home knocking over lamps and cabinets alerting everyone within ear shot of their presence.

Examples of Telerik Exploits in Recent Cases

Kroll responded to one example incident in which an e-commerce client had a downstream customer report instances of fraud after using a credit card on their website. In early May, after several days of review, the client found a malicious script that captured cardholder data (more specifically it captured content of the visitor's typed in or auto-filled check out form input) upon checkout. The client assessed that the Telerik vulnerability had been exploited to introduce the malicious script. They removed it, but by that point, the script had impacted a significant number of cards due to the client's daily e-commerce site traffic. The Kroll team proposed validating the scope of the client's exposure, conducting a root cause analysis and reviewing logs to determine whether any additional scripts or web shells were introduced.

In another investigation, a Kroll client started receiving complaints from customers whose banks informed them that fraudulent charges were originating from the client organization. A couple weeks before the attack, one of the client's IT vendors advised that they had identified the Telerik vulnerability within their vendor-managed database, which allowed code to be remotely executed in an unauthorized manner. The Kroll team proposed conducting an investigation into unauthorized access of data contained in or entered into the client's website and to review systems for possible acquisition of same.

Another client had cryptomining software deployed in their environment. The Telerik vulnerability was used to upload malicious files and run malicious binaries allowing the escalation of privileges in an Internet Information Services account from an internet accessible server. With elevated privileges, the actor(s) retrieved cached credentials from system memory using tools such as Mimikatz which allowed further access the network, lateral movement between servers and eventual staging and deployment of the XMRig cryptocurrency mining software.

Micheal Quinn
Managing Director

Devon Ackerman
Managing Director

Kroll Experts Corner:
Best Practices for Preventing Telerik Exploits

The following recommendations, provided by Kroll experts Michael Quinn and Devon Ackerman, should be taken into consideration to prevent exploits directed at the Telerik vulnerability:

- Enforce a consistent vulnerability and patch management program focusing on internet-facing infrastructure
- Conduct periodic penetration testing or red team exercises
- As mentioned in several of our previous articles, deploy multi-factor authentication for all internet-accessible remote access services
- Ensure adequate Windows event logging and forwarding and system monitoring is in place
- Update Telerik UI to the latest version available. Telerik is also included with third-party software, such as the last case Kroll worked on. In this instance, third-party vendor software should be updated and remain in contact to ensure the vendor is aware.
- Search for the version of Telerik if unknown. This can be accomplished using tools such as grep, PowerGrep or the "strings" binary. If Telerik can be updated, isolate the host, bring offline or monitor the system more thoroughly.
- Look for connections to the following URL within the web server logs: /Telerik.Web.UI.WebResource.axd?type=rau

Leave Nothing to Chance

Managing an ever-expanding list of vulnerabilities takes considerable resources and it's especially hard to determine which vulnerability deserves priority attention. For internal teams burdened with a host of other priorities and a remote workforce, support from dedicated experts who have the frontline expertise, resources and technical skills to assess your exposure can greatly reduce your risk profile. Talk to a Kroll expert today via our 24x7 hotlines or contact form.

CVE-2020-10189: Zoho ManageEngine Vulnerability Still Dangerous Nearly a Year Later

Zoho ManageEngine Desktop Central is an endpoint management solution offered by Zoho. A server running this software can push updates to managed systems, remotely control and lock them, apply access controls and more.

In March 2020, a remote code execution (RCE) vulnerability was identified (tracked as CVE-2020-10189) in the ManageEngine software due to the deserialization of untrusted, user-controlled input in the getChartImage function of the FileStorage class within the application. An unauthenticated user can exploit this vulnerability to gain code execution with the same permissions as the ManageEngine software.

One of the reasons for the ongoing importance of this vulnerability is the fact that it is commonly used by managed service providers (MSPs) as part of their offerings to clients. If an MSP is running a vulnerable version of ManageEngine (earlier than 10.0.474), exploitation of the vulnerability potentially provides access to all of their customers' networks and devices.

Why This Vulnerability is so Critical

CVE-2020-10189 receives a common vulnerability scoring system (CVSS) 3.x score of 9.8. This means that the vulnerability is labeled as "critical" based upon potential exploitability and impact, for several reasons:

- **Unauthenticated RCE:** The vulnerability exists in publicly-exposed functionality. This means that any unauthenticated user can access a vulnerable server exposed to the internet and achieve remote code execution.
- **Elevated Permissions:** Exploitation of this vulnerability enables an attacker to run commands on the vulnerable server with SYSTEM permissions. This is the highest level of permissions on Windows systems and enables the attacker to perform nearly any action on the system.
- **Device Management:** The ManageEngine software is designed to enable centralized management of a number of devices on the network. Exploitation of a single server provides the ability to push updates, remotely control and control access of all managed devices.

When the vulnerability was published in March 2020, approximately 2,300 instances of ManageEngine were publicly exposed on the internet. This is likely an underestimate of the number of potentially vulnerable machines as some will have been deployed to be only accessible internally. However, for these internal devices, compromise of a single device on the network could enable exploitation of the vulnerability to gain control of all managed devices.

CVE-2020-10189 Remains Relevant

CVE-2020-10189 received a patch the day after its publication, but nearly a year later this vulnerability remains relevant, thanks to its flexibility and recent involvement in a data breach in which a red team toolkit was exposed. This vulnerability is one of several used by this toolkit, meaning CVE-2020-10189 has gained new visibility and less sophisticated cyber threat actors now have the ability to effectively exploit it. This exploitation has been demonstrated several times, through commercial, off-the-shelf applications where the domain controller of a system was manipulated. Threat actors have left system disks intact but encrypted other drives through a connected service account. To prevent an infiltration like this, it is important to ensure that if a service account is needed, it runs with minimal privileges.

Examples of ManageEngine Exploits

In one of our recent ransomware engagements, Kroll investigators identified the exploitation of the ManageEngine remote code execution vulnerability on March 8, 2020, three days after the vulnerability was published. The threat actor utilized the Windows Background Intelligent Transfer Service (BITS) to download a malicious batch file from a virtual private server hosting provider. The threat actor utilized Cobalt Strike to facilitate lateral movement within the client's network and solidified their foothold by creating a scheduled task that would run daily to download and install the software. Soon after executing a network enumeration tool on two domain controllers to identify hosts on the client's network, the threat actor began encrypting endpoints.

Scott Zuberbuehler
Vice President

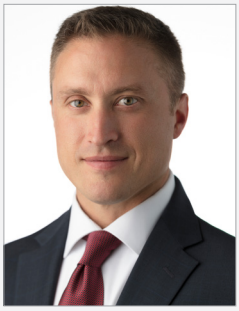
Kroll Experts Corner:
Protecting Against CVE-2020-10189

This vulnerability only exists in versions 10.0.474 and earlier. Updating affected software will close the vulnerability. Additionally, configuring firewall rules and access controls to minimize access to the affected server can help to limit the exploitability of this and other potential vulnerabilities in the software.

Security professionals can find powerful resources to help their teams stay up to date with new vulnerabilities from MITRE and NIST.

It's important to remember there are many legitimate reasons for a company to keep an unpatched vulnerability in place for business or operational reasons. Maintaining a program that can monitor and understand the impact of new vulnerabilities to determine how soon to patch requires considerable resources, beyond what many smaller teams can undertake. A mature cyber security program would balance vulnerability management investments with a stronger ability to detect and respond to incidents, which provides a more robust defensive posture.

Contact Us



Keith Wojcieszek
Managing Director, Cyber Risk
keith.wojcieszek@kroll.com | +1 443 295 5082

Based in Washington, D.C., Keith joined Kroll from the United States Secret Service, where he served with distinction for 15 years. Most recently, Keith led the USSS Cyber Intelligence Section, Criminal Investigation Division, where he managed the agency's national response to cyber investigative initiatives focused on protecting the financial infrastructure of the United States. In this role, Keith also coordinated complex international investigations that targeted transnational organized crime networks with an emphasis on cyber and information security.

Nicole Sette
Senior Vice President, Cyber Risk
nicole.sette@kroll.com | +1 609 514 8225

Based in the Secaucus office. Nicole is a highly accomplished security professional, who brings unique insight to the multiple dimensions inherent in client challenges from her years of federal law enforcement and military experience. Nicole served as a Cyber Intelligence Analyst with the Federal Bureau of Investigation for nearly 10 years, and was an Intelligence Specialist with the U.S. Army Communications-Electronics Command for four years.

Browse the latest editions of *The Monitor* and subscribe free at kroll.com/themonitor

About Kroll

Kroll is the world's premier provider of services and digital products related to governance, risk and transparency. We work with clients across diverse sectors in the areas of valuation, expert services, investigations, cyber security, corporate finance, restructuring, legal and business solutions, data analytics and regulatory compliance. Our firm has nearly 5,000 professionals in 30 countries and territories around the world. For more information, visit www.kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Duff & Phelps Securities, LLC. Member FINRA/SIPC. Pagemill Partners is a Division of Duff & Phelps Securities, LLC. M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Duff & Phelps Securities Ltd. (DPSL), which is authorized and regulated by the Financial Conduct Authority. Valuation Advisory Services in India are provided by Duff & Phelps India Private Limited under a category 1 merchant banker license issued by the Securities and Exchange Board of India.