Kroll | A Division of DUFF & PHELPS

The MONITOR

VOLUME 1

Business Email Compromise Trends and Mitigation

Kroll identified 25 business email compromise (BEC) incidents during the month of January 2019 alone, marking a growing trend. Among the BEC incidents that Kroll reviewed, representative attacks led to unauthorized changes to direct deposit information, unauthorized mail forwarding and fraudulent wire transfers of up to $5 million.

BEC incidents most commonly involved an actor compromising an Office 365 Outlook account. For example, Kroll reviewed an incident where a human resources employee complained to her payroll department that her banking information had been changed. Payroll investigated and found an email record from the employee requesting the change. Upon further investigation, the company discovered unauthorized logins to the employee's Office 365 account from an external IP address. A malicious actor had likely obtained her Office 365 credentials and was able to use her email account to request a change in banking information.

Corporate executives are under particular assault by BEC attackers. Managing Director Jonathan Fairtlough explains, "Criminals are focusing their efforts on executives not only because of their access to high-value data, but also their reach throughout the entire enterprise. Companies should back up executive training with technology that provides early detection of problems to reduce the opportunity for lateral movement once a hacker breaches their systems."

Jonathan continues: "While senior executive accounts are commonly targeted, it is important to note that any employee routinely accessing customer account data or treasury functions is at risk."

BEC attacks also continue to be highly lucrative for cybercriminals in the form of wire transfer fraud. According to the FBI, in 2018 nearly 21,000 victims lost close to $1.3 billion. "Wire fraud highlights a persistent security weakness — our human nature. In the cases we've seen, when employees receive requests from senior executives, the motivation to assist the person higher in rank outweighs the need to stop and validate that the request is legitimate" says Peter McFarlane, Managing Director and Toronto Office Head.

According to Peter, tone from the top is critical for combating this crime: "A company's most senior managers need to make it absolutely clear to everyone involved in approving wire transfers that no one, no matter their rank, can override policies or proper procedures."

Technically Speaking

The growing adoption of Microsoft Office 365 requires specialist skills in securing and/or investigating the environment in the event of BEC and insider threats. Check out these Kroll resources for insights to help you better meet the challenges ahead:

- **A Planned Methodology for Forensically Sound IR in Office 365.** First presented at SANS DFIR Summit 2018, this talk by Managing Director Devon Ackerman discusses numerous forensic, incident response and evidentiary aspects of Office 365. Based on two years of forensics and incident response data collection in Microsoft's Office 365 and Azure environment, it also encompasses more than a hundred Office 365 investigations, primarily BEC and insider threat cases. View now.
- **Penetration Testing for Active Directory Forests: Exploring Trust Relationships.** Active Directory (AD) is a critical software for most organizations in that it serves as the single centralized point for handling authentication and authorization control access to all critical resources within an organization. As Kroll's security penetration testing lead Carlos Garcia discusses in this article, compromise of just one domain admin account in the AD forest could give an attacker unrestricted access to all resources managed by all domains, users, servers, workstations and data. Read more and download slides here.

Case Studies

As these recent Kroll cases demonstrate, BEC incidents are not going away and warrant ongoing vigilance.

- Hackers sent a legitimate-looking phishing email from an account belonging to one large company's Director of Corporate Services to approximately 900 external recipients and 400 internal recipients at that company. In this case, any of those emails could have been used to initiate unauthorized BEC transactions.
- A supervisor at a financial services company received an email request from a business associate at another financial institution. Despite recognizing the request was somewhat out of character, the supervisor – who routinely works with financial information – opened the attachment expecting an invoice. The document was in fact a maliciously crafted document which triggered a chain of events on the endpoint that were invisible to the user.

BEC Red Flags for Wire Fraud

Unusual or vague transaction details.
The transaction is described in vague terms (e.g., "strategic marketing advice") or referenced as a confidential matter known to senior management (e.g., "confidential joint venture investment"). Instructions regarding recording of the transaction are also vague (e.g., "corporate marketing").

Unknown beneficiary and round-sum amounts.
The beneficiary is typically a person/entity unknown to the organization and may reference a jurisdiction in which the organization typically does not conduct business. Round-sum amounts, such as "$200,000," should raise suspicions, although many fraudsters are aware of this and often avoid them.

Absence of required supporting documents.
Normal wire transfer requests should be supported by appropriate documentation available to both those preparing and approving the transfer. Fraudulent requests often state supporting documents will be provided later or were provided to the CEO or other senior executives.

Non-standard email format.
Any irregularity in email headers, footers and content such as John.Doe@acme.com rather than the standard format jdoe@acme.com or use of an atypical font or email footer suggest that it could be a fraudulent communication (in addition to a false email domain).

Requirement to circumvent normal protocols.
A pretext is often presented to justify the need and urgency to circumvent normal protocols. These include reasons such as the funds must be received before end of business the next day to close a confidential transaction, avoid penalties or avoid seizure of product.

Kroll Experts Corner:
Mitigating Business Email Compromise

Following are some insights from Kroll experts on how to prevent or mitigate the harms from business email compromise.

Implement Multifactor Authentication
Requiring that all users- especially senior and treasury staff use a multi factor authentication system to access email is the most effective mitigation step to take. A phishing attempt or credential theft can be effective, but without the additional token or access method, the attacker cannot access the mailbox.

Review Email system Configuration
Email systems need to be properly configured and regularly reviewed. There are many modern security processes to securely configure an email system like Office 365 to enforce trusted relationships with common clients and partners, and to track and block misuse. A security professional needs to review email configurations, regularly log and review the use of forwarding rules, domain trust settings, and external exchange access.

Phishing Training
Implement regular phishing awareness training and consider implementing testing to review how many users within the organization are clicking on phishing links. Phishing emails can be used to compromise network credentials and carry out BEC attacks against your organization.

Beware of social media links
Recent open source reporting highlights an increase in phishing emails designed to look like LinkedIn updates with titles like "profile views" and "InMail message". These emails can be used to harvest credentials for use in BEC scams. Train employees to use caution when opening these types of messages in their corporate mail accounts.

Raise awareness of spoofed domains
Hackers will often buy a domain that is similar to a vendor or client's name but will change one letter or spell the name differently. Employees in payroll and other finance departments should receive training on how to recognize spoofed domains or emails; additionally, create protocols for double-checking domain names and email accounts to ensure the accounts match up to the legitimate company name and domain.

Implement dual verification procedures for financial transactions, including wire transfer requests
Many BEC attempts rely on creating a sense of urgency or presenting a business case that pressures the targeted individual to quickly transfer funds or edit banking information, so the attacker can swiftly carry out fraudulent activities. Ensure mechanisms are in place to validate requests before action is taken, such as predefined escalation protocols. Also, build a corporate culture that stresses defined channels and protocols cannot be circumvented by anyone, no matter how senior.

Ryuk and the Resurgence of Ransomware

Kroll identified 15 ransomware cases in the month of February 2019, with a particular presence of the Ryuk variant in the majority of investigations. we noted the highly opportunistic Ryuk variant seizing on vulnerable networks, with attacks across industry sectors, including manufacturing, government, education, professional services and healthcare.

Kroll reviewed Ryuk ransom notes that directed victims to contact a Swiss-based ProtonMail email address. Then the attackers followed up with varying demands for payment in bitcoin. Based on our experience and other reports, most Ryuk ransomware attacks follow this pattern.

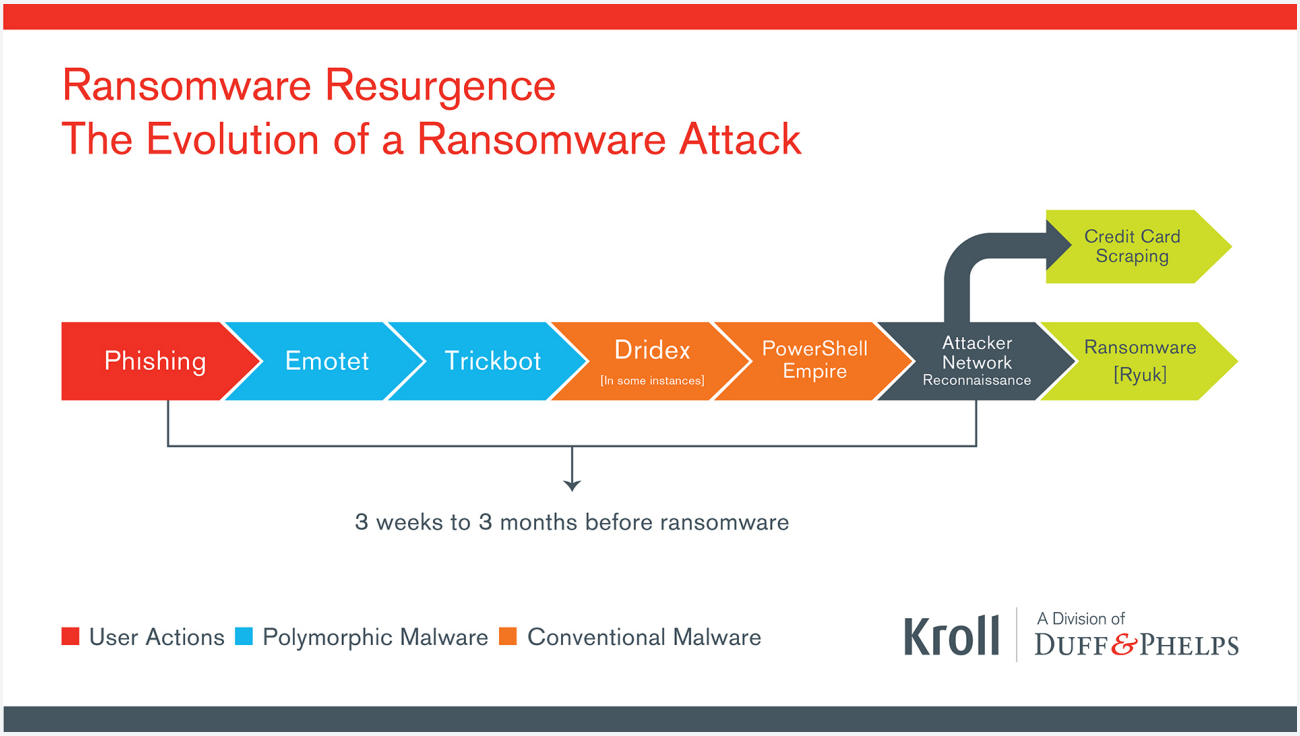
However, Ryuk mainly differs from other ransomware families based on its delivery mechanism. Most types of ransomware rely on phishing attacks or open Remote Desktop Protocol (RDP) connections. Ryuk most often leverages established command and control servers associated with Trickbot and Emotet banking trojans. This allows the Ryuk attackers to access a large swath of victims and "cash in" on high-value Trickbot and Emotet victims; they then tailor ransom demands to each organization. *(See the **Technically Speaking** section in this newsletter for a representative attack sequence.)*

While Ryuk attackers profit from their ties with these trojans, the connection also provides a tripwire that can alert victims to a potential ransomware attack following a trojan infection. "Ransomware in 2019 is significantly different than ransomware in 2017, with attackers leveraging the access gained with Trickbot and Emotet, which usually includes domain administrator access. Attackers now spend far more time performing reconnaissance on an impacted network, which allows them to have a high level of confidence that an organization will have to pay the ransom. We have identified attackers deleting backups to make recovery increasingly difficult," says Associate Managing Director Pierson Clair.

Pierson continues, "Most trojans are introduced via methods such as social engineering attacks, specifically infected email attachments. Emotet and Trickbot are families of polymorphic malware, which makes them very difficult for anti-virus to identify. However, we know these attack vectors can be addressed effectively with several other proven measures. These range from human-focused efforts, such as educating employees and making social engineering exercises part of broader technical penetration testing programs, to implementing layers of technological solutions, including threat intelligence and endpoint detection and response applications. So, organizations can virtually head off Ryuk at the pass by implementing best practices that prevent Trickbot/Emotet from getting a foothold in the first place."

Technically Speaking

Following is a typical sequence of events that Kroll's investigations have identified in the evolution of Emotet/Trickbot/Ryuk attack.



According to an FBI Flash, the Ryuk ransomware variant is marked by these characteristics:

- First appeared as a derivative of Hermes 2.1 ransomware and became available on the open market as of August 2018
  - Retains some aspects of Hermes code; all of Ryuk's files contain the "HERMES" tag, but some of the files have .ryk added to the filename, while others do not
  - In other parts of the ransomware code, Ryuk has removed or replaced features of its predecessor
- Ryuk deletes all files related to the dropper used to deploy the malware
  - Ryuk has been deployed secondary to Trickbot and/or Emotet banking Trojans, which use Server Message Block (SMB) protocols to propagate through the network and can be used to steal credentials
- After the initial attack, additional network exploitation tools may be downloaded, including PowerShell Empire, the Microsoft Sysinternals tool psexec, or the penetration testing tool Cobalt Strike
- Once executed, Ryuk establishes persistence in the registry, injects into running processes, looks for network connected file systems, and begins encrypting files
- Ryuk utilizes AES-256 to encrypt files and uses an RSA public key to encrypt the AES key.
- The Ryuk dropper drops a .bat file which tries to delete all backup files and Volume Shadow Copies (automatic backup snapshots made by Windows), preventing the victim from recovering encrypted files without the decryption program

Kroll Experts Corner:
Mitigating Ransomware

Following are some insights from Kroll experts on how to prevent or mitigate the harms from a ransomware attack, including the Ryuk variant.

Backups, backups, backups
If ransomware does strike, and backups are valid and intact, then recovery is significantly easier. However, Managing Director Devon Ackerman cautions that organizations might be operating under a false sense of security in their backups. "While many organizations have robust processes for creating backups, a similar rigor often doesn't extend to validating the security controls around the backups. For example, is the backup on an open network? Could a breached domain admin credential access the backup? These issues and more all leave open the possibility that an attacker could destroy the backup repository."

Conduct routine security risk assessments, including vulnerability and penetration testing
Preventing trojans from entering and taking hold in your organization will go a long way toward neutralizing the Ryuk ransomware threat. Addressing fundamental cyber risks through expert assessments and targeted testing can help prevent your organization from being victimized twice. Tabletop exercises can also be instructive; practice incident response scenarios that include complex attacks combining disruption through ransomware, DDoS, network downtime, etc.

Implement endpoint monitoring, detection and response
Solutions such as Kroll's CyberDetectER® Endpoint prevent the spread of the attack by halting the execution of the code that launches the encryption processes before it damages and cripples systems.

Use a firewall to prevent all public access to the Service Message Block (SMB/port 445) and the Remote Desktop Protocol (RDP/port 3389).
Remote access should be restricted to a dedicated server that requires multi-factor authentication (MFA), which ensures sufficient privilege access restriction and logging capability.

Configure file integrity monitoring
File integrity monitoring should also be configured to monitor file creations in trusted locations, like the System32 directory. This can also be used to monitor deletes, with an alert configured to fire on excessive deletes in a row.

Boosting Your Insider Threat Program: Examples, Indicators, and Mitigation Steps

In March, nearly one in five of all Kroll's Cyber Risk engagements were insider threat incidents, most commonly affecting the healthcare and financial service industries. Kroll reviewed cases that involved former employees gaining unauthorized access to data, as well as current employees inadvertently exposing confidential data.

According to the New Jersey Cybercrime Communications and Integration Cell (NJCCIC), "Insider threats can include current or departing employees, contractors, third party vendors, technicians, business partners, and anyone granted administrator privileges. If organizations do not have the right preventative measures in place and management is not cognizant of the indicators of an insider threat, they are putting themselves at great risk."

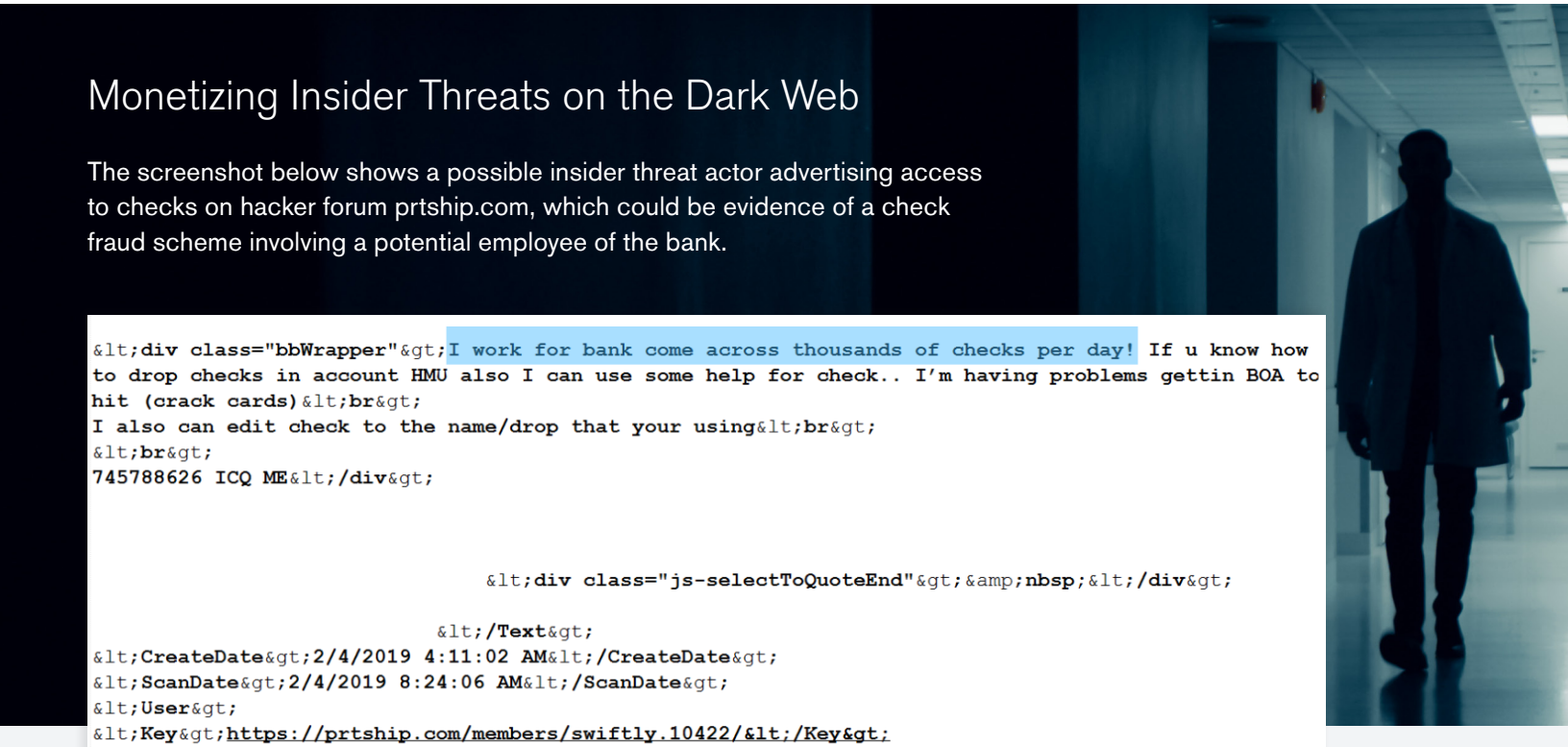
Insider threat incidents involving former employees are increasing as companies move proprietary information to cloud-based services. Departing employees with active credentials (their own or those of a co-worker) pose a threat to even the most secure networks, as the examples below highlight:

- In a recent incident covered in open source news reports, a disgruntled former employee at a UK-based firm stole a coworker's credentials and deleted 23 of his former company's cloud servers.
- A New Jersey woman stole trade secrets from her employer, posting the stolen material on the website of a Chinese subsidiary company, of which she was part owner. She admitted to accessing an internal company database and downloading information related to chemical compounds onto her employer-issued laptop. She then transferred the information to her personal home computer by sending it to her personal e-mail address or via a USB thumb drive.

Cases like these demonstrate the high-impact nature of some insider threat investigations. It is imperative that organizations deploy procedures to make it as difficult as possible for departing or disgruntled employees to have access to active credentials which can be used to exfiltrate sensitive data or access key internal systems.

Monetizing Insider Threats on the Dark Web

The screenshot below shows a possible insider threat actor advertising access to checks on hacker forum prtship.com, which could be evidence of a check fraud scheme involving a potential employee of the bank.




```
&lt;div class="bbWrapper"&gt;I work for bank come across thousands of checks per day! If u know how
to drop checks in account HMU also I can use some help for check.. I'm having problems gettin BOA to
hit (crack cards)&lt;br&gt;
I also can edit check to the name/drop that your using&lt;br&gt;
&lt;br&gt;
745788626 ICQ ME&lt;/div&gt;



                                &lt;div class="js-selectToQuoteEnd"&gt;&amp;nbsp;&lt;/div&gt;

                            &lt;/Text&gt;
&lt;CreateDate&gt;2/4/2019 4:11:02 AM&lt;/CreateDate&gt;
&lt;ScanDate&gt;2/4/2019 8:24:06 AM&lt;/ScanDate&gt;
&lt;User&gt;
&lt;Key&gt;https://prtship.com/members/swiftly.10422/&lt;/Key&gt;
&lt;Name&gt;Swiftly&lt;/Name&gt;
```


Kroll Experts Corner:
Mitigating Insider Threats

Following are some insights from Kroll experts on how to prevent or more quickly detect data exposure caused by insiders

Don't let your business outgrow your security

Businesses of all sizes need to carefully weigh their exposure, but quick-growing or complex enterprises can particularly find the team overdriving technology, leaving some gaping security holes. If your business is expanding or in the midst of other organizational changes, consider deploying technical resources (e.g., endpoint threat monitoring or third-party cyber risk management solutions) and dedicated in-house staff or contract with outside resources (such as a virtual CISO) to help keep your business safe. Significant changes in size, through organic growth or acquisition should be seen as a trigger to update your risk assessment.

Make security part of workflows to promote sustainability

Assess how your employees really work and then use that knowledge to put in place the right rules, tools and compliance mechanisms. For example, in Kroll's latest Global Fraud & Risk Report, security experts Alan Brill, John Friedlander, and Jonathan Fairtlough described how an organization could provide each outside salesperson with a tablet complete with paid cellular access. Customer data and forms are stored in a document management system in the cloud, and the tablet has mobile device management software that blocks all browsing. If lost, the device is encrypted and can be remotely wiped. No local storage, no vampire data or data hoarding.

Establish and maintain defensible data access policies

For example, an "Acceptable Use of Information Technology Policy" should reflect and communicate rigorous controls the organization has established for employees and third parties regarding the proper use of its systems, data and resources. These can include practices such as requiring employees to use only company-approved devices and systems as well as restrictions on using social networking sites and non-corporate email on company devices. Of course, in setting these rules, you must be serious about compliance, as the rules represent what is in effect a promise of what you're going to do to protect information.

When employees depart, immediately restrict physical and electronic access

Preferably before an employee permanently leaves the premises, make sure to deactivate, disable or delete network account access (both local and remote), ID authentication tokens, security codes, email accounts and access cards. Because malicious insiders can leverage "forgotten access" to enterprise applications, the use of a single sign-on (SSO) solution can help close this gap. Also, try to determine if the individual would have access to the credentials of other employees and if so, re-set those as well.

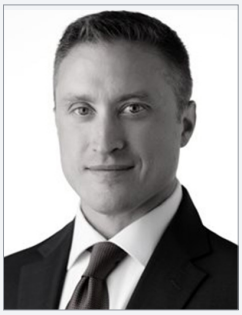
Employ technology that can "look beyond your borders" for at-risk data

In professional circles, it is common knowledge that for some industries, engineers and others are using chat rooms on the dark web to specifically sell and buy intellectual property and trade secrets. Sophisticated solutions such as Kroll's CyberDetectER® DarkWeb continuously monitors this activity and acts as an early warning system that sensitive proprietary data could be compromised.

More best practices to address insider threats, by Senior Managing Director, Alan Brill:

- Set the tone from the top and promote a corporate culture where "cybersecurity is everyone's responsibility."
- Apply the principle of least privilege: Limit network access to those who need it for their jobs.
- Restrict the use of removable media.
- Integrate checks of cybersecurity program elements into your internal audit and compliance programs to assure that they are working as intended.
- Consider data loss prevention (DLP) processes designed to prevent data loss holistically, including DLP products, company policies, user training, internal reviews, and more.
- Watch for early warning indicators that include remote access during off-hours, unexplained exporting of large amounts of data and never taking a vacation.
- Regularly scan your network and generate an automated inventory of all IoT devices that are connected. Investigate any entries that cannot be accounted for to ensure no "mystery" devices are attached to your network

Contact Us



Keith Wojcieszek
Associate 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
Director, 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.

Kroll | A Division of DUFF & PHELPS

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

About Kroll

Kroll is the leading global provider of risk solutions. For more than 45 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security and data and information management services. For more information, visit www.kroll.com.

About Duff & Phelps

Kroll is a division of Duff & Phelps, a global advisor with nearly 3,500 professionals in 28 countries around the world. Our clients include publicly traded and privately held companies, law firms, government entities and investment organizations such as private equity firms and hedge funds. We also advise the world's leading standard-setting bodies on valuation and governance best practices.

For more information, visit www.duffandphelps.com.