verizon

BROWNRUDNICK

Risk intelligence advisory:

Threats to client data in the legal services sector.

March 2016: Verizon security teams have identified an elevated threat level affecting the legal services industry (NAICS 54). The sector is being targeted at a far higher frequency than normal and companies should be on high alert for the threat indicators listed in this advisory. We expect further attacks in the short term, with some leading to confirmed data breaches. Successful breaches will almost certainly attract more threat actors to target the sector.

This advisory is a synopsis of the threat intelligence compiled by Verizon on the recent spike of attacks within the legal services sector. It relates to the theft of sensitive client intellectual property as well as client funds. The Verizon RISK (Research, Investigations, Solutions, Knowledge) Team has first-hand knowledge and reliable intelligence on an exceptionally high number of security incidents that have occurred over the past 180 days. We expect many of the attacks we've seen in this period to be confirmed as data breaches.

Threat actors have demonstrated two main objectives when targeting law firms and e-discovery consultancies. Thefts have focused on client intellectual property, and client trust and escrow funds. In both cases, attacks typically involve social engineering of employees of the targeted firm as the initial point of intrusion.

Like our Data Breach Investigations Report (DBIR), this advisory is organized using the VERIS framework. We also offer some guidance to help you harden your defenses, spot attacks and limit the damage caused.

While this information is focused on law firms and e-discovery consultancies, it's also relevant to organizations within the professional services industry – since they store a comparable level of client data and have similar clients. Most business-to-business (B2B) companies can benefit from this advisory, especially those handling third-party data, funds on behalf of others (such as estates and trusts) and other types of sensitive data.

Read the 2015 DBIR to learn more about how to prioritize your defenses. Download >

Become an Insider to get early access to our reports, including the 2016 DBIR. Sign up >

Speak to one of our specialists to find out more about our portfolio of security services. Contact us >

How to identify attacks: frequently observed characteristics.

Victim assets

Which assets were affected?

The attacks we've seen primarily targeted the theft of sensitive client intellectual property, attorney-client privileged communications and client funds.

The systems most significantly impacted were end-user workstations, centralized file server repositories and e-discovery review platforms.

Most attacks used a combination of corporate and bring your own device (BYOD) assets. And initial entry points were often end-user systems, such as desktop workstations and laptops.

Threat actors

Who were the perpetrators?

Our assessment, supported by related evidence, is that cybercriminals in Eastern Europe and Asia are responsible for the majority of these attacks.

The RISK Team has determined that some attacks were almost certainly perpetrated by the same threat actors. Where intellectual property and attorney-client privileged data were targeted, evidence most commonly points to threat actors operating in Asia. Organized crime groups in Eastern Europe were considered most likely to be responsible for cases that targeted client, escrow and settlement funds.

Attributes

How was the asset affected?

The threat actors installed and ran malware, created files and directories, and modified email configurations and mailboxes.

Threat actions

What actions affected the asset?

Based on the common methods and the overlapping timeframes of the attacks, the threat actors appear to have targeted several victims simultaneously. In most cases, the threat actors used spear phishing campaigns to gain end-user credentials. Evidence suggests individuals with more active social media accounts were targeted.

The threat actors then attempted to access the firm's VPN or web-based email platform. In all cases we've seen so far, the victims were not employing two-factor authentication. This made the use of stolen credentials a relatively straightforward task.

Threat actors pursuing intellectual property and attorney-client privileged communications typically harvested, culled and forwarded large quantities of emails. In addition, they extracted and exfiltrated data from file servers and e-discovery review platforms. In some cases, threat actors established email-forwarding rules to automate exfiltration and continue the process even if the compromised credentials were later changed.

The threat actors pursuing client, escrow and settlement funds typically used the VPN to connect to end-user workstations. Once connected they installed keylogging malware to capture URLs, usernames and passwords. Captured credentials were then used to manipulate the associated financial accounts and issue fraudulent payments.

Telltale indicators

Unusual remote access – multiple, simultaneous remote access sessions, especially if from two different or unusual locations.

Abnormal email activity – excessive email activity that appears scripted or email-forwarding rules containing external-destination addresses.

How to combat attacks: preventative countermeasures.

Establish baselines and visibility

Define "normal". Create and maintain an inventory of assets so you can prioritize the protection of high-value data. Establish security baselines for email gateways, e-discovery platforms, remote access systems and the networks that these systems use. This will enable you to recognize and react to anomalies; some of which may indicate an attack.

Detect the suspicious. Review use of your existing logging capabilities. Have a process to routinely review and archive logs. Add effective monitoring to help eliminate blindspots and improve visibility of key components within your email infrastructure, e-discovery environments and remote access facilities. Monitor incoming and outgoing traffic, and related access points.

Increase scrutiny of third parties

Right to audit third parties. Ensure that you have the contractual right to audit third parties that provide your legal, e-discovery and other professional services. Many service industries lack clear guidance on data security. Trust but verify – and make sure you conduct periodic audits. The same goes for third-party forensic investigations.

Breach notification by third parties. The underlying data compromised in these breaches is typically the property of a client (i.e. third-party data). It is imperative that the owner of the data includes breach notification language in all contracts to ensure that they receive adequate notice should a breach occur.

Security awareness and education. Breach scenarios involving social engineering are widely considered as weaknesses in the human element. Ensure that you and your third parties are aware of your security policies, conduct regular awareness training and education, and test the effectiveness of your measures.

Improve your access control

Require two-factor authentication. Especially for remote access and entry to critical systems. Two-factor authentication should also be considered for important communications tools, such as web-based email.

Restrict email forwarding. Restrict the ability of end-users to create email rules that automatically forward their corporate email to external destinations. Flag for review any email forwarding to external addresses that exceeds agreed velocity thresholds.

Single remote sessions. Remote access via VPN or web-based email platforms should be limited to a single concurrent connection. This will help reduce the likelihood of various types of credential exploitation and make such an attack more immediately obvious.

Plan and test your incident response

Be prepared. Consider suffering a breach as inevitable and prepare accordingly.

Establish reporting procedures. Start with how you handle reports of anomalies, suspicious events and known indicators of compromise.

Designate an expert team to handle potential incidents. Set thresholds for escalating notifications of in-progress inquiries. When in doubt, notify the Investigative Response (IR) team(s) and preserve evidence.

Test your readiness. Run periodic rehearsals to validate that your IR team has the skills, tools and equipment to preserve evidence of a breach.

Plan when to pull the plug. Have a decision-making process in place to decide when an incident merits disconnecting systems.

A lawyer's perspective.

Stephen R. Cook, Partner at Brown Rudnick

In the legal profession, we're entrusted with our clients' most sensitive secrets. Protecting this information is a key part of the attorney-client privilege.

Beginning in law school, lawyers are taught that the attorney-client privilege is sacrosanct. Under its protection, clients share with us their most sensitive, most valuable and – in some cases – incriminating secrets. Unfortunately, many law firms' cyber defenses do not match the value of the secrets they protect.

> Law firms hold a lot of sensitive documents about their clients. They are not just potential, but likely targets for those looking to find sensitive information.
>
> Craig Silliman, Verizon General Counsel

Recently, there have been a number of wake-up calls. For example, when a group of hacktivists breached a global entertainment company, they released gigabytes of personally-identifiable information, intellectual property and – to the horror of lawyers everywhere – confidential legal advice.

Some of these attorney-client communications revealed the existence of a previously confidential government investigation – news of which landed on the pages of the Wall Street Journal and Forbes. Although in this case the breach was not of the lawyers' network, it serves as a cautionary tale for anyone working in the legal industry.

As the traditional targets of cyber attacks strengthen their defenses, hacktivists and cybercriminals are seeking out paths of lesser resistance to the same confidential data. Those routes often involve law firms, e-discovery providers and other professional advisers that have not previously considered themselves to be high-value targets.

It is vital that law firms and other advisers with access to confidential information recognize that they face the same threats as their clients and take action to protect themselves against cybercriminals. That includes not only appropriate technical defenses, but a developed situational awareness on the part of lawyers to the exposure threat facing their clients' confidential data.

BROWNRUDNICK

Stephen Cook, a partner at Brown Rudnick, is a former federal prosecutor and experienced trial lawyer who advises corporate and individual clients on complex civil and criminal matters, internal corporate investigations, cybersecurity/ cyber-incident preparedness and regulatory compliance matters.

Verizon and Brown Rudnick have developed an unified and industry-leading services portfolio, which couples the breadth of Verizon's technical security consulting expertise with Brown Rudnick's global cybersecurity legal advisory services and crisis management experience. www.brownrudnick.com

verizonenterprise.com