Kraft Kennedy

A DAY IN THE SECURITY OPERATIONS CENTER

The threats law firm security analysts are fielding every day

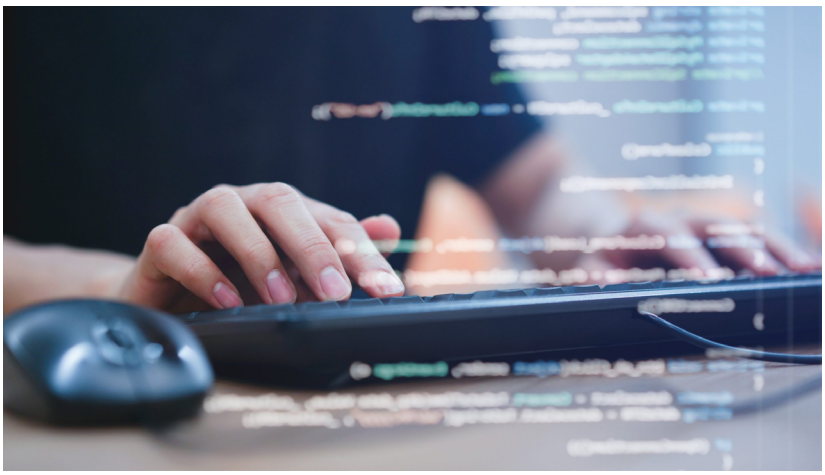
JOHN KOGAN

A DAY IN THE SECURITY OPERATIONS CENTER

The threats law firm security analysts are fielding every day

by **John Kogan**

John Kogan is the Chief Information Security Officer of Kraft Kennedy. Based in a round-the-clock Security Operations Center, his team of expert security analysts provides ongoing security monitoring and incident remediation to law firms of all sizes.



If you monitor the computers of six thousand law firm users, you will see a staggering number of hacking attempts. We know because that is how many people our Security Operations Center (SOC) is currently defending.

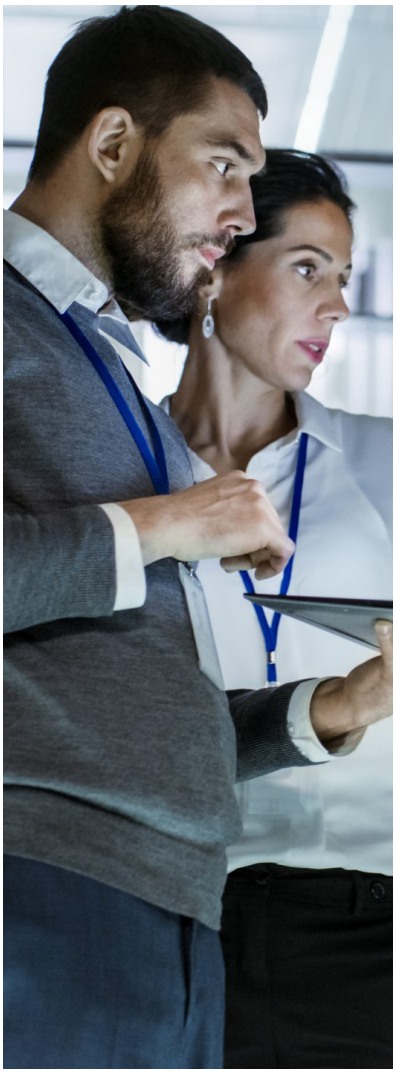
Here is a behind-the-scenes look at what the Kraft Kennedy security analysts do daily to keep our clients from potential disaster.

EMAIL: DECEPTIVELY SIMPLE

Hackers try to get into firms via various doors. The number one entryway, by far, is email. Much of our day is spent, specifically, fielding phishing emails: filtering and blocking attempts and mitigating the effects of successful attacks.

On the face of it, phishing may seem like an unsophisticated form of attack: a faked email, often with misspellings and other telltale signs, tries to entice users into clicking on a link, opening a file, or giving up their credentials in a bogus log-in window (these can actually look quite convincing). But, in fact, the vast majority of cyber-intrusions at law firms occur via this method. For this reason, we always recommend that our clients let us configure email hygiene and maintenance systems with strong filtering rules. These systems block an estimated 95% of incoming attacks. Some firms, wary of legitimate emails getting caught by the filters, insist on looser rules, and more harmful emails make it through as a result.

Despite our best filtering efforts, a few such emails do manage to reach end-users. Once alerted to the presence of a phishing attempt, we put into place our phishing-fighting process. We ascertain the email's recipients, determine who clicked on the link, and identify anyone who



may have mistakenly given away their credentials. We then clean the affected devices, scanning them for a malicious presence or evidence of a payload—that is, the thing the hackers are after—such as a connection to a server made by an unauthorized party. We encounter many false positives every day. Most of the alerts we receive for email and other systems turn out to be nothing. But we must analyze them all. It only takes one successful hacking attempt to bring down a law firm.

THE PAYLOAD

What are these shadowy actors after?

Credentials, as mentioned, are a much sought-after treasure. Hackers often sell them in bulk. Buyers use them to hack into an enterprise and personal accounts, which often use the same username and password combinations.

Hackers are also out to install viruses or other malicious code such as ransomware. Users afflicted with ransomware get a message that their documents are locked up until a ransom is paid. Sometimes, we've found, the threat is empty; though the message says so, the documents are not in fact locked up, but we have seen cases in which the "victim" pays the ransom anyway. In other cases, files really are hijacked. In that case, firms should revert to backups, if they have them (we maintain current backups for all our clients).

Clandestine crypto miners are an increasingly popular illicit installation. Bitcoin mining is an example of a wide-net, automated algorithm. Bitcoin mining consists of siphoning off computing resources—electricity, power, memory—to create Bitcoins. The routine runs across the internet, looking for the pieces it needs. It takes a long time; the programs collect cents worth of resources at a time and one Bitcoin, at the time of this writing, is worth $37500. By setting up farms consisting of many unsuspecting users' computers and leaving them to run, stealing resources, Bitcoins are eventually "mined."

COMBATTING MALWARE

Using our console at the SOC (think NASA-style setup), we monitor six thousand client-computers for malware and viruses. We see them become infected throughout the course of the day.

Our anti-malware algorithms flag abnormalities. We clean them up and investigate the cause, looking at network packets, which give us a breadcrumb trail of what's going on in the environment. We validate them

and then perform remediation. At the Security Operations Center, this is all routine. But it's not something most Help Desk Analysts are equipped to do. Having specially trained security experts on staff is, therefore, one of the main advantages of a SOC. Analysts have usually completed formal courses of study in cybersecurity that provide a foundation of knowledge and allow them to keep up with evolving security threats.

POLICY

Setting and enforcing policies is a significant aspect of our job. This goes beyond Group Policy and documented guidelines and rules to include monitoring of alerts by our team. For example, we:

- Isolate administrator accounts. Users with full administrative privileges are cordoned off from everyone else at the firm. This goes a long way toward containing damage in the event of a breach.

- Disable the keyloggers that come with Windows. This is not as simple as flipping a switch to shut off the capability across the firm—doing so can cause interdependent applications to go down—and involves granular fine-tuning.

- Investigate excessive log-in attempts. We are alerted when there have been multiple failures to log on to a firm-owned property. While this can be merely a user who has forgotten a password, it is also often the sign of a brute-force attack in which an automated process repeatedly tries to guess a password.

WEB-FILTERING

Along with email filtering, web-filtering is a critical component of basic security hygiene to prevent the intrusion of malicious actors.

Web-filtering entails keeping a "blacklist" of disallowed websites. As with email, firms

have different preferences for how strict they prefer their filter. If they make it too tight, then legitimate, needed emails and websites might get caught in the net; too loose, and users will have to field all manner of traps. Skewing toward tighter filtering is, from the standpoint of security, better. While users may find themselves occasionally inconvenienced, it beats suffering a massive breach.

A surprisingly wide array of websites make it onto blacklists. It's not just the gambling and adult websites. Sometimes legitimate websites might be prone to infection. Any website is liable to infect others. HTTPS won't protect you. Hackers can, via the hosting platform, install a "drive-by file," that, once a user inadvertently clicks on it, will be installed on their computer.

At the SOC, we maintain web-filtering systems with daily updates to a list of websites known to be compromised. Ironically, cybersecurity websites are often infected. Hackers love to target those looking to stop them.

DARK WEB BREACH INTELLIGENCE

In addition to monitoring compromised websites, we maintain a current database of breaches. This daily preventative SOC activity is referred to as "Dark Web Breach Intelligence."

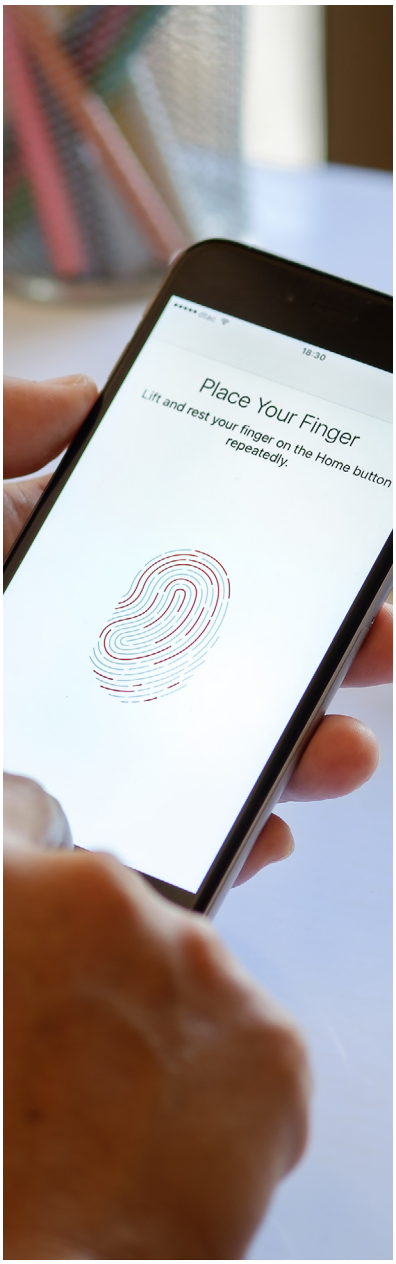
Many people use their work email addresses to sign up for other websites. Many of these people use the same username and password combinations for these sites as well (one reason why password policies requiring a minimum length and regular changes are a good idea). If one of these websites is breached, these firm credentials might go for sale on the black market. For instance, if you use your work email for your Amazon account, and Amazon suffers a breach in which credentials are exposed (this has not, to our knowledge, actually happened), your firm might be vulnerable as a result. When a breach occurs, we see when one of our six thousand users has used their work account to sign up, and we prompt them to change their passwords.

We also stay apprised of advisories from the National Vulnerability Database and the Department of Homeland Security, which send out preemptive warnings. One governmental alert, for example, recently warned us that Iran was poised to use "cyber offensive activities" to steal intellectual property and personally identifiable information (PII), spread malware, and target U.S. infrastructure such as power, light, water, and internet.

INTRUSION DETECTION

Intrusion detection is another of our go-to tools. It can reveal a great deal. The presence of shadow IT for one, including the use of unauthorized repositories like Dropbox, unapproved applications, or the exfiltration of data via USB.

We can also see the presence of foreign, unauthorized machines on the network. This lets us know that a hacker has connected to the firm's network and needs to be expelled.



BEYOND THE DAY-TO-DAY: ONGOING MAINTENANCE AND PREVENTATIVE ACTIVITIES

Aside from our daily activities of maintenance, prevention, and remediation, the SOC conducts other regularly scheduled work for our clients.

On a monthly basis, we scan for vulnerabilities and apply newly released patches to switches, firewalls, UPS devices, wireless devices, and anything else that touches the internet or can be a vehicle to enter the client's environment. We also implement other important preventative activities, such as security awareness training and multi-factor authentication (MFA) for devices and applications.

WHO'S BEING TARGETED?

How do intrusions happen, you may ask, despite all the aforementioned precautions have been put in place?

The truth is that if someone is intent on hacking a firm, they will get in, despite the defenses. Typically, attacks on law firms are not targeted. Hackers cast a large net, often using automated processes. If they manage to glean access or credentials, they put them up for sale on the dark web.

Sometimes, though, firms are targeted. Usually, this is because they are engaged in financial transactions, have political connections, or deal with intellectual property. Burisma, the Ukrainian company connected with the Bidens and President Trump's impeachment trial, is one such target. It was subject to a large-scale—successful—phishing attack. More often, specific law firms make appealing victims for their role in transferring client funds.

Should one of our clients be targeted, the SOC will be there to defend and remediate. ■

kraftkennedy.com
hello@kraftkennedy.com
(800) 523-3081