Securities Litigation Alert

Akin Gump
STRAUSS HAUER & FELD LLP

SEC's Examination Function Warns Its Registrants of Risks Associated with Dangerous Malware

July 15, 2020

Key Points

- In the age of broad corporate teleworking brought on by COVID-19, OCIE of the SEC has observed during recent examinations that investment advisers, broker-dealers and investment companies are subject to an increased threat of ransomware attacks.
- In a July 10 Risk Alert, the latest in its series of cybersecurity-related alerts, OCIE highlights several practices and procedures that it suggests may limit or prevent exposure to ransomware and other information security vulnerabilities.
- This Risk Alert follows on the heels of another alert issued by OCIE on June 23, 2020, warning RIAs of compliance deficiencies observed during recent OCIE examinations. Taken together, these Risk Alerts warn of OCIE's expected focus in upcoming examinations, and all SEC registrants should ensure their cybersecurity policies and procedures meet regulatory standards and sufficiently protect against the growing threat of ransomware that OCIE has observed.

Introduction

For the past eight years, the Office of Compliance Inspections and Examinations (OCIE) has included information security as a key element of its examinations. On July 10, 2020, OCIE released a Risk Alert regarding the increasing frequency and sophistication of ransomware attacks targeting U.S. Securities and Exchange Commission (SEC) registrants. The Risk Alert highlights best practices to protect against and respond to ransomware attacks.

Ransomware Threat Increases

Ransomware is a type of malware that infects a computer or network and encrypts the system's critical data until the victim pays a ransom to regain access. According to Beazley, one of the leading insurance carriers in the cybersecurity space, the use of ransomware increased by 25 percent in the first quarter of 2020.[1] OCIE notes in the Risk Alert that it has recently observed increased ransomware attacks targeting SEC registrants—i.e., broker-dealers, investment advisers and investment companies—as well as their third-party service providers. Specifically, the Risk Alert underscores the

Contact Information

If you have any questions concerning this alert, please contact:

Peter I. Altman
Partner
paltman@akingump.com
Los Angeles
+1 310.728.3085

Michael A. Asaro
Partner
masaro@akingump.com
New York
+1 212.872.8100

James Joseph Benjamin Jr.
Partner
jbenjamin@akingump.com
New York
+1 212.872.8091

Paul W. Butler
Partner
pbutler@akingump.com
Washington, D.C.
+1 202.887.4069

Charles F. Connolly
Partner
cconnolly@akingump.com
Washington, D.C.
+1 202.887.4070

Jason M. Daniel
Partner
jdaniel@akingump.com
Dallas
+1 214.969.4209

Estela Díaz
Partner
ediaz@akingump.com
New York
+1 212.872.8035

threat of Dridex malware, one of the most frequently used financial Trojans, being used specifically against the financial sector.[2]

This Risk Alert is the second alert OCIE has released concerning a particular malware variant. The first was issued in 2017 following the widespread WannaCry ransomware attack, which affected organizations in more than 100 countries. OCIE's particular warning about Dridex therefore is significant and must be heeded with great caution.

To combat ransomware like Dridex, OCIE encourages registrants to stay up-to-date with alerts released by other government agencies, including the DHS Cybersecurity and Infrastructure Security Agency (CISA) and by the FBI's Internet Crime Complaint Center (IC3). OCIE references CISA's June 30, 2020, update concerning Dridex, which explains in technical detail how threat actors often utilize email phishing campaigns to inject Dridex malware into network systems, particularly those in the financial services industry. CISA's update also includes a robust list of mitigation recommendations to combat Dridex tactics, techniques and procedures (TTPs).

Approaches to Combat Ransomware

Some of the Risk Alert's recommendations that home in on ransomware include:

- **Access Rights and Controls**: The Risk Alert identifies numerous access control best practices to limit threat actors' ability to penetrate a system via ransomware. These best practices include restricting user access to the least privileged access possible at all times and removing that access immediately upon termination of employment or an engagement, implementing access protections such as strong password requirements and multifactor authentication, and controlling, monitoring and reviewing access approvals and privileges. OCIE also advises that registrants pay particular attention to the access rights of those with heightened privileges, such as administrators and service accounts.
- **Training and Awareness**: Email phishing is one of the key methods utilized by threat actors to deploy ransomware on a system. OCIE notes that financial institutions have increasingly been the targets of phishing campaigns, and encourages registrants to ensure their employees are sufficiently trained to identify potential phishing attacks and maintain heightened awareness of potential threats.
  - OCIE likely calls attention to phishing because there has been a significant increase in phishing attacks overall in 2020. Threat actors have largely used the coronavirus as a means to exploit unwary employees who may have more lax cybersecurity hygiene while working from home.
- **Incident Response and Resiliency**: The Risk Alert suggests that registrants should assess, test and periodically update their incident response plans (IRPs) and make sure these plans address ransomware and other denial of service attacks. OCIE also encourages registered investment advisers (RIAs) to ensure their IRPs include up-to-date procedures for complying with state and federal data breach notification and reporting laws and for notifying relevant parties, potentially including regulators, law enforcement and/or customers.
- **Data Loss Prevention**: OCIE highlights the need for operational resiliency, including the ability to access a secondary system to continue to operate critical applications if the primary system becomes unavailable due to a ransomware attack. The Risk Alert further emphasizes that registrants should implement

Katherine Rachel Goldstein
Partner
kgoldstein@akingump.com
New York
+1 212.872.8057

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Mark J. MacDougall
Partner
mmacdougall@akingump.com
Washington, D.C.
+1 202.887.4510

Claudius B. Modesti
Partner
cmodesti@akingump.com
Washington, D.C.
+1 202.887.4040

Parvin Daphne Moyne
Partner
pmoyne@akingump.com
New York
+1 212.872.1076

Douglas A. Rappaport
Partner
darappaport@akingump.com
New York
+1 212.872.7412

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Jacqueline Yecies
Partner
jyecies@akingump.com
New York
+1 212.872.7479

Molly E. Whitman
Counsel
mwhitman@akingump.com
Los Angeles
+1 310.728.3737

Jenny M. Walters
Senior Practice Attorney
jwalters@akingump.com
Dallas
+1 214.969.4654

© 2020 Akin Gump Strauss Hauer & Feld LLP

vulnerability and patch management programs and keep them updated to prevent ransomware attacks.

- OCIE emphasizes that registrants should back up their data and keep it geographically separated in case of an attack.
- Notably, the Risk Alert also pinpoints perimeter security as a key tool in preventing ransomware attacks and advises that registrants employ best practices for use of Remote Desktop Protocol (RDP) through an encrypted virtual private network (VPN). With a high percentage of the American workforce working from home, RDP presents a significant vulnerability for ransomware attacks.
- Maintaining security capabilities to closely monitor all traffic through tools such as firewalls, intrusion detection systems, email security capabilities and web proxy systems with content filtering is also noted as a key practice to reduce ransomware threats.

Conclusion and Recommendations

We recommend that registrants review the full list of identified best practices and procedures in the Risk Alert to avoid becoming the next victim of a ransomware threat and, further, that registrants share this alert with third parties that hold their data—especially administrators. With this alert, OCIE has signaled that how registrants control and respond to ransomware attacks will continue to be a focus of OCIE examinations.[3] OCIE referrals remain a common source for the opening of investigations by the Division of Enforcement, and registrants should thus pay close attention to the Risk Alert.

Registrants should also consider implementing the following measures, or reviewing existing measures for required updates, in addition to those OCIE identified:

1. Institute other best practices concerning RDP, including disabling RDP where it is not required, as RDP is one of the network features most vulnerable to a ransomware attack.
2. Establish procedures that make it simple for employees to immediately report suspicious emails and attachments. For example, implement a button within your email client to automatically forward a suspicious email to the designated IT response team, or create an easy-to-remember email account to which employees can send questionable communications.
3. Configure firewalls and other perimeter security capabilities to block known malicious IP addresses and other identified indicators of compromise (IOCs).
4. Require multifactor authentication for all network access.
5. Contact outside counsel as soon as possible if data loss is known or suspected to ensure the greatest protection of investigation materials and conclusions under the attorney-client privilege.
6. Extend all policies and procedures to cover personal devices that are capable of accessing the organization's network.

[1] https://www.beazley.com/news/2020/beazley_breach_insights_june_2020.html.

[2] Earlier this year, Dridex was included for the first time in Check Point Research's Global Threat Index as one of the top ten most prevalent malware variants, and the third most prevalent during March 2020. See

© 2020 Akin Gump Strauss Hauer & Feld LLP

https://www.globenewswire.com/news-release/2020/04/09/2014156/0/en/March-2020-s-Most-Wanted-Malware-Dridex-Banking-Trojan-Ranks-On-Top-Malware-List-For-First-Time.html.

[3] That this is the second OCIE alert in recent weeks advising registrants to keep a watchful eye out for deficiencies in their controls, policies and procedures emphasizes that registrants must proactively monitor their compliance ahead of potential OCIE examinations. See our Client Alert discussing OCIE's observed deficiencies during private investment fund adviser examinations for more information.

akingump.com

© 2020 Akin Gump Strauss Hauer & Feld LLP