MICROSOLVED,INC.

Business Email Compromise Checklist

Overview:

In modern life and business, email has become a foundation service. We use it for everything from personal communications to day to day operations. Often, the contents of our email inboxes and folders have a great deal of private information and can often be used by attackers to commit fraud, wreak organizational havoc or cause immense amounts of reputational damage.

These attacks, often referred to as Business Email Compromise or “BEC”, for short, have become quite common in the last several years. Attackers routinely target email systems and trade in compromised email accounts. At MSI, we have worked many of these security incidents and prepared this checklist to help organizations with the scourge of BEC.

Common Attack Vectors

Several common attack vectors have emerged for targeting email credentials. They are as follows:

- **Phishing** - Attackers have become quite adept at replicating webmail logins for most common webmail systems - including cloud hosted webmail services. They often lure users to a site that appears to require their webmail credentials and then harvest that information for re-use against real webmail deployments.
- **Password Re-Use** - Attackers research their intended targets and identify sets of previously compromised login credentials available on the web, or in the dark net markets. Once they have a set of known credentials for likely users, they attempt to re-use those credentials (and common variants) against exposed webmail deployments and other authentication portals looking to gain access.
- **Malware** - Attackers may install malware on user’s systems at work, at home or their mobile devices to gain access to email credentials.
- **Public Wi-Fi Attacks** - Use of insecure public Wi-Fi networks can lead to email credential exposure. Attackers can capture or intercept credentials during user activity, even if that activity is automated and unobserved - such as from a mobile device or phone that is misconfigured to join untrusted networks without notification.
- **Social Engineering** - Many users have fallen victim to a variety of social engineering schemes such as remote technical support, vendor calls or text messages, etc. These attackers simply trick users into disclosing their credentials for illicit purposes.

Impacts

Once an attacker has gained illicit access to an email account, they often leverage that access to dig through the email contents and exposed information for data that they can resell or reuse. Forms, business process information, other authentication credentials, consumer identity data and anything else of value are quickly stolen. Any exposed business processes, especially those associated with money movement (wire, ACH, etc.) are usually attacked for fraud within hours. Once they have stolen the data they want, they often use the account to phish or infect other victims inside the organization or to attack business partners.

Control Suggestions Mapped to NIST Model:

While BEC is a significant issue and a common form of compromise leading to fraud, there are several things you can do to combat this form of attack. Some suggestions are detailed below, mapped to the NIST model for information security.

Identify

- □ Identify and catalog all of the authentication portals where attackers could test stolen credentials or leverage them for access.
- □ Catalog and socialize the systems involved in mail processing and in offering webmail access, especially if these systems are cloud-based or hosted off-premise.
- □ Identify and flag similar or suspicious domains that could be used for spoofing or to trick users into revealing credentials.
- □ Implement a system for users to alert the security team on suspicious email activity and a mechanism to alert users to emerging attack patterns as they happen against your organization.
- □ Review log settings for webmail systems and ensure that they will capture the appropriate information needed during an incident - including remote IP, details of what was accessed, outgoing mail activity, etc.
- □ Make sure that someone with appropriate access to perform email log analysis, authentication analysis and make control changes is available at all times. Have a backup staffing plan in place for long incident timelines. Socialize this information as appropriate.

Protect

- □ Implement Multi-Factor Authentication (MFA) wherever possible, but especially for remote access to webmail, VPN and other critically sensitive services. Proper MFA is the most significant preventative control against BEC.
- □ Consider restricting access to Internet-facing webmail services to specific IP ranges, or requiring remote users to be logged into a VPN to gain access to the service.
- □ Implement heavy scrutinization for any process that moves money, or that would suffer from email exposures, and routinely audit it against best-practices.
- □ Implement keyword filtering/highlighting for common fraud terms in email bodies and add a subject tag such as [EXTERNAL] to all emails originating outside the domain.
- □ Implement appropriate email filtering, anti-malware and phishing detection controls.
- □ Routinely conduct phishing exercises with various content and forms of trickery to better maintain user awareness and tune your prevention and detection systems in an ongoing manner.
- □ Provide ongoing user training about the risks of email compromise and how to report suspicious account and email activity. Have them pay special attention to requests for secrecy and/or urgency in transactions.

Detect

- □ Review logs and email authentication detections at least daily. Look for abnormal login times, unusual locations or abnormal usage patterns and investigate them when found.
- □ Pay careful attention to emails that have a sender and receiver in your domain, but have an external reply-to address. Ensure that these are flagged for review and alert the user visually to the potential risk.
- □ Periodically check user configurations for unexpected auto-deletion or forwarding rules, which are common signs of compromise. Even better, ensure that creation of new rules are logged and provide alerting to the appropriate admin staff for review.
- □ Pay attention to user reports of password lockouts or other email access oddities. Investigate these to ensure that an attack is not currently in progress.

Respond

□ Capture, review and archive all appropriate logs and alert messaging.
□ Notify management or other teams as appropriate
□ Catalog each suspicious account throughout the process and immediately suspend the account and/or change the credentials. Be aware that attackers may attempt to reset passwords, especially if automated.
□ Scan for location information, unexpected IP addresses, suspicious subject and email body contents, etc. across the domain.
□ Review and investigate each potentially compromised account. Don't assume that the attacker(s) performed the same actions on each account. When you find new Indicators of Compromise (IOCs), scan for them against the entire domain.
□ Audit each account for outbound email activity and issue email recalls, or alert additional parties as needed and as appropriate in accordance with organizational policies.
□ Check each account for email forward, auto-deletion and other automation rules. Note and delete any unexpected rules, using them as IOCs.
□ Note and catalog all suspicious email data including from, reply-to, IP addresses, subject, unusual wording or phrasing, links, graphics, etc. Use these as IOCs for further investigation across the domain.
□ If wire fraud or other monetary transaction attacks have been performed, take appropriate steps to notify law enforcement, initiate SWIFT recall messages, perform wire recall processes, notify involved banks of the issue and request cooperation with your team and law enforcement as needed. Double check all wire and ACH information, including receiving bank, routing numbers, etc. to ensure that they are as expected. Consider a period of call-back verification for any transactions in doubt, or from impacted accounts.
□ Pay particular attention to any email requests to change payment types, payment terms, or locations that originated during the incident, especially from impacted accounts.
□ Inform impacted employees of the issue and ask for their ongoing vigilance for other problems stemming from the incident or if they observe other unexpected behaviors.

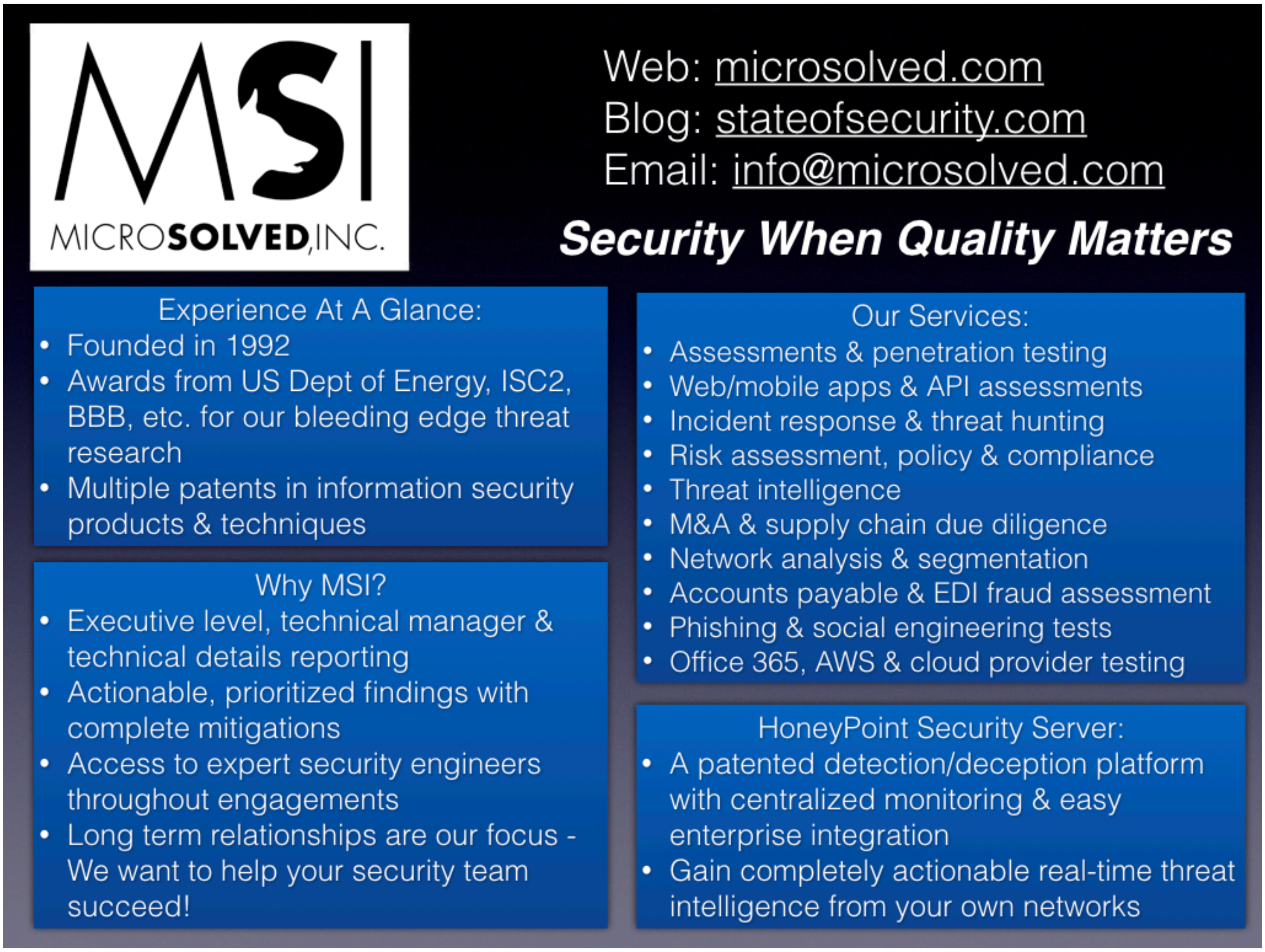
Recover

□ Regardless of damages, please report the activity to the FBI at http://www.ic3.gov.
□ Prepare any reports and notifications required by regulation, law or policy and deliver as appropriate.
□ Prepare lessons learned reports and socialize as appropriate according to your site's incident response policies.
□ Share incident details and lessons learned with appropriate management, board-level or committee level members.
□ Implement any additional controls to minimize the risk of future attacks.

More Information:

- FBI rates BEC as a 5 billion dollar criminal industry - https://www.ic3.gov/media/2017/170504.aspx
- BEC impacts across 5 years from the IC3 - https://www.ic3.gov/media/2018/180611.aspx

About MicroSolved, Inc.:



MICROSOLVED, INC.

Web: microsolved.com
Blog: stateofsecurity.com
Email: info@microsolved.com

Security When Quality Matters

Experience At A Glance:

- Founded in 1992
- Awards from US Dept of Energy, ISC2, BBB, etc. for our bleeding edge threat research
- Multiple patents in information security products & techniques

Why MSI?

- Executive level, technical manager & technical details reporting
- Actionable, prioritized findings with complete mitigations
- Access to expert security engineers throughout engagements
- Long term relationships are our focus - We want to help your security team succeed!

Our Services:

- Assessments & penetration testing
- Web/mobile apps & API assessments
- Incident response & threat hunting
- Risk assessment, policy & compliance
- Threat intelligence
- M&A & supply chain due diligence
- Network analysis & segmentation
- Accounts payable & EDI fraud assessment
- Phishing & social engineering tests
- Office 365, AWS & cloud provider testing

HoneyPoint Security Server:

- A patented detection/deception platform with centralized monitoring & easy enterprise integration
- Gain completely actionable real-time threat intelligence from your own networks

Thanks for reading and if you found this helpful, please let us know.
We appreciate feedback on Twitter @MicroSolved or drop us a line - info@microsolved.com.

If we can be of any assistance or if you need help regarding a business email compromise or other security issue, feel free to give us a call - (614) 351-1237.

Version 1.0