Credential theft – the Monster Cache

2018 Data Breach Digest

verizon

The situation

Cybersecurity trends continue to show that organizations most often learn of data breaches through external, third-party notifications. In recent years, the information security industry has integrated cyber threat intelligence into cybersecurity and breach response strategies.

The VTRAC | Cyber Intelligence Team monitors the cyber threat pulse 24x7 for our global customers, leveraging cyber threat intelligence capabilities such as: consistent monitoring of the DarkNet (that "not-easily-accessible" part of the internet used for anonymized content sharing), subscribing to threat intelligence feeds, and incorporating databased indicators of compromise from historical incidents.

With this continued growth and reliance on cyber threat insights, the VTRAC cyber intelligence analysts provide customers with proactive mitigation measures and reactive response actions for data breaches. A normal day in the life of a VTRAC cyber intelligence analyst includes frequent requests from our customers asking to "tell me what I don't know."

Mitigation tips

- Keep current on the cyber threat landscape and the threat actions targeting your industry
- Integrate threat intelligence into operations and facilitate threat data dissemination

All successful breaches can be presented as threat actor goals, capabilities and methods. This perspective enables the creation of attack models. When combined with organization profiling, unique risk reporting is possible and can be a valuable input for both strategic and tactical decision-making. It's with this perspective in mind that our cyber intelligence analysts approached the onboarding of a new Rapid Response Retainer Service (RRR) customer one particular afternoon.

Investigative response

Here, the organization operated in an industry frequently targeted by espionage-oriented threat actors who rely heavily on phishing emails as an initial vector. The emails usually seek to entice recipients into providing user name / password combinations for external access points, using methods such as carefully crafted phishing content and links to enticing, yet compromised, watering-hole websites.

Detection tip

Review logs to learn how threat actors are targeting your organization; consider creating honeypots to detect, counteract, and gain insight into targeted attacks.

When we look at the data sold and traded by cyber criminals, stolen credentials are at the top of this list. For opportunistic attackers, this data is sometimes all they need to further an attack on an organization.

During initial DarkNet monitoring efforts, we typically expect to see all sorts of compromised information available on the criminal underground. However, we were surprised to discover a dump of over 500 corporate user account identifiers and password combinations available in a DarkNet forum. No sooner had we reported our findings than we learned other persons in that same organization had engaged our VTRAC | Investigative Response Team to investigate the unauthorized use of an employee's email account.

Investigators performed a forensic examination to analyze threat actor activity associated with the compromised accounts, and report back with significant information relevant to the case. Mail transfer logs associated with the email accounts were examined, along with the phishing email itself, and our threat research was utilized to uncover its origin and provide important context around the threat actor group.

Response tip

Upon being notified of user credential compromise, change them immediately!

Implement $+r0^g passwords

After compromise, reset passwords for all user accounts. Implement a strong password policy that includes:

- Assign all users separate, unique accounts – don't use generic or shared accounts or passwords
- Set first-time passwords to a unique value for new users; require password lengths of at least eight (8), preferably more, alpha-numeric-special characters
- Change user passwords immediately after the first use and then at least every 90 days
- Block historical passwords from being used for at least the previous four (4) utilized passwords and set the lock-out threshold to six (6) times
- Remove / disable inactive user accounts at least every 90 days; immediately revoke access for terminated users

The findings indicated the activity stemmed from a compromised user account from which additional phishing emails were sent internally to much of the end user population. The malicious message included an embedded link to a credential-harvesting site, prompting users to authenticate via username and password.

Lessons learned

Threat intelligence alone may not always be a perfect predictor of data breaches, but the insight provided from modeling attacks and attackers should be considered when making security decisions. The process enables stakeholders to see how threat actors view their organization and provides responders with possible focus areas when scoping cybersecurity incidents. Aside from sensitizing end users to recognize and report email phishing attempts, three recommendations for mitigation, detection, and response are:

Mitigation and prevention

- Keep current on the cyber threat landscape and threat actions targeting your industry
- Integrate threat intelligence into operations and facilitate threat data dissemination

Detection and response

- Review logs to learn how threat actors are targeting your organization; consider creating honeypots to detect, counteract, and gain insight into targeted attacks
- Upon being notified of user credential compromise, change them immediately!

Look what I can do: the myriad "values" of stolen credentials

Every day, newly harvested login credentials are bought and sold on underground DarkNet forums and marketplaces. While most of these fall into the category of services like streaming media and personal email, the impact of a stolen username / password combination goes far beyond someone watching the latest must-see series on your favorite streaming app.

Here are a few of the damaging after effects seen in our 2017 casework, which is limited only by the creativity of the perpetrators:

- Compromised remote admin app credentials led to RAM scraper malware installation on point-of-sale (PoS) systems. Dozens of retail locations were affected, resulting in numerous payment card data breaches
- Admin accounts credentials harvested from an exploited, externally accessible database allowed attackers to install multi-featured web shells. Within a matter of minutes, sensitive data was being shipped out to systems operating on The Onion Router (Tor) network
- Compromise of an admin account led to numerous follow-on account thefts via credential stealing malware. The highly privileged access rights of the initial account facilitated lateral movement within the network and ultimately resulted in sensitive personnel files being exfiltrated
- The unauthorized use of accounts in a company's finance department gave threat actors unfettered access to vendor payment information. Multiple fraudulent payments were issued prior to detection, resulting in a lucrative transfer for the criminals
- Ever popular webmail phishing campaigns prompted dozens of unsuspecting employees in one company to divulge their login information. Then the self-service payroll accounts of these individuals were accessed and direct deposit information changed, netting the attacker sizable paychecks for a hard day's work