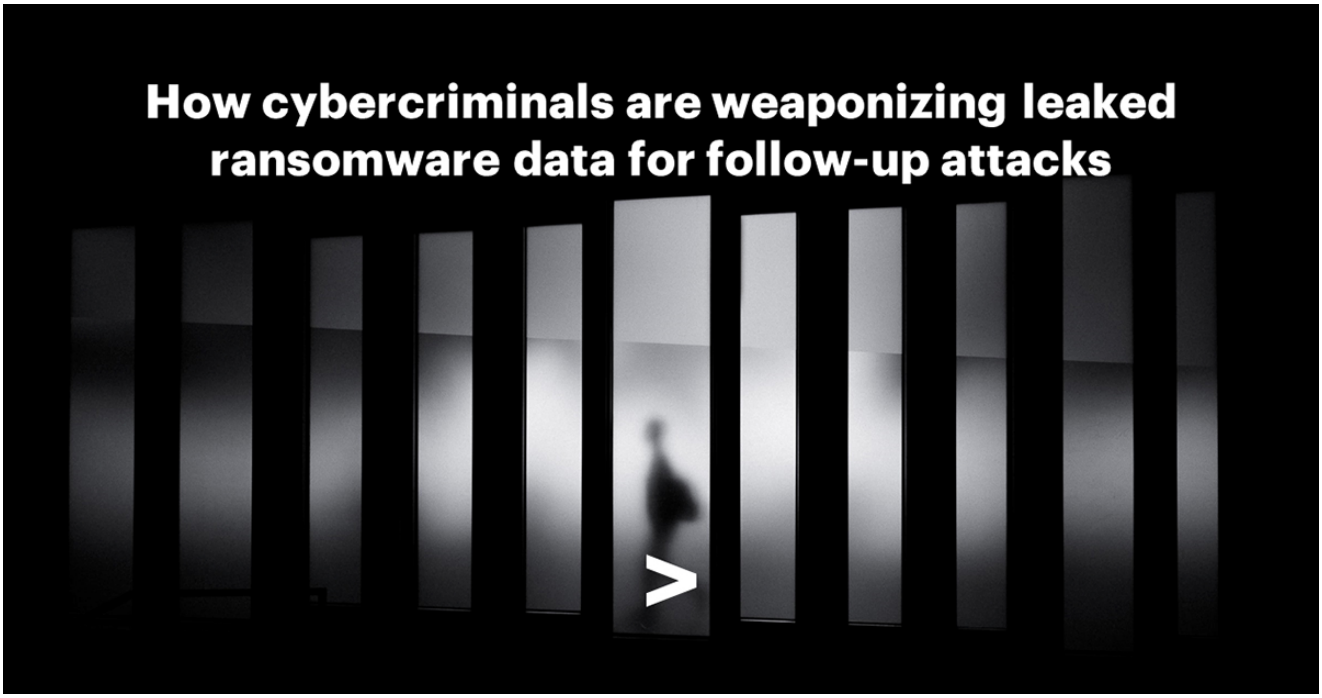
How cybercriminals are weaponizing leaked ransomware data for follow-up attacks

accenture.com/us-en/blogs/security/cybercriminals-weaponizing-leaked-ransomware-data



Security
Cyber Defense

August 11, 2022

Share

Business email compromise (BEC) is becoming a more sophisticated cyber threat because of the availability of sensitive corporate data on the dark web. This is problematic, as BEC and its derivates, such as vendor email compromise (VEC) and invoice fraud, are the largest categories of malicious activity in terms of monetary losses. In 2021, victims lost an estimated $2.4 billion to BEC scams, totaling more than a third of all cybercrime losses ($6.9 billion) and causing more losses than ransomware attacks, according to FBI estimates.

The widespread use of ransomware with the use of data disclosures (together sometimes known as double extortion) has made sensitive corporate data highly available on the criminal underground, with such data available for free or a fee to any threat actor. The data

is a rich source of information for criminals who can easily weaponize it for secondary BEC attacks. This is especially relevant, as markets like Genesis and underground services available in multiple high-end forums allow malicious users to purchase credentials for as little as $10 that provide access to genuine corporate email accounts. This helps attackers launch a BEC attack from an internal, genuine email address as opposed to a spoofed address an attacker would otherwise use. Such use of genuine email addresses makes it increasingly difficult for businesses and consumers to distinguish malicious activity from genuine business operations.

Data disclosures

The Accenture Cyber Threat Intelligence (ACTI) team analyzed data from ransomware leak sites and compared its own research with that of external entities. ACTI examined the top 20 most active dedicated leak sites, or dark web name-and-shame sites, measured by number of featured victims, between July 2021 and July 2022 (Exhibit 1). Within this period, ACTI observed an estimated 4,026 victims (corporate, non-governmental organizations and governmental entities) on various ransomware groups' dedicated leak sites.

<<< Start >>>

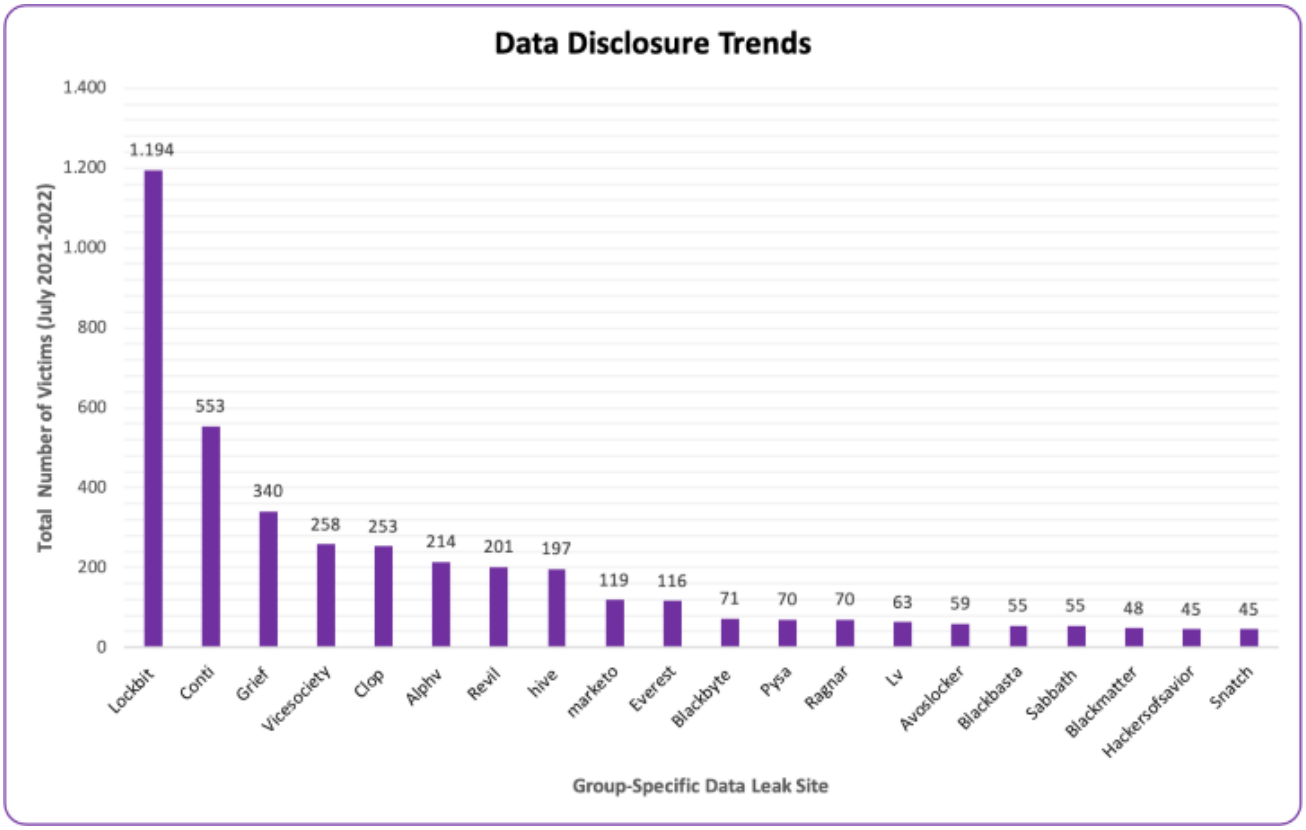


Exhibit 1: Breakdown of data leak victims on dedicated leak sites

<<< End >>>

An estimated 91% of the 4,026 victims on dedicated leak sites incurred subsequent data disclosures of various degrees, with the remaining victims not having experienced an observed data leak. The notion that nearly all ransomware collectives, regardless of size, engage in double-extortion techniques indicates that malicious actors disclose very large amounts of data, making that data available to anyone.

ACTI has found that dedicated leak sites most commonly provide financial data, followed by employee and client personally identifiable information, and communication documentation. These findings echo the observations of other researchers. ACTI also found that whenever an exfiltrated batch of data includes at least one of the above categories, the group that exfiltrated it consistently highlights the data type on its dedicated leak site. This boasting showcases the perceived high value of such data and the propensity for the disclosure of such data. The highlighted section of Exhibit 2 provides an example of such promotion from RedAlert's dedicated leak site.

<<< Start >>>

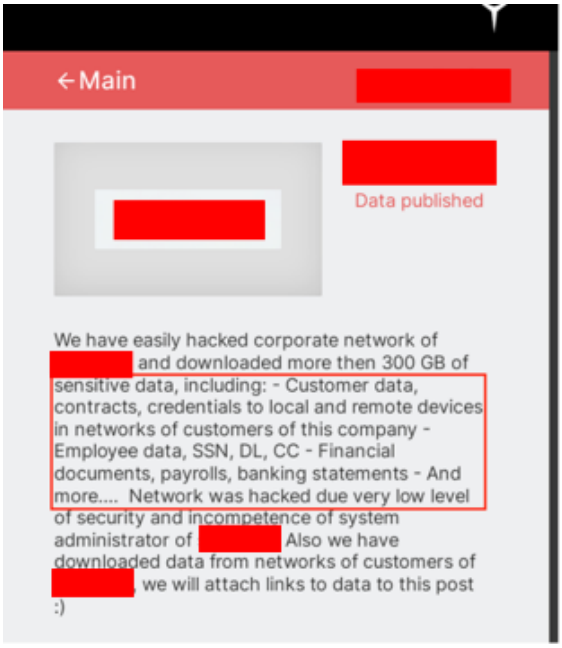


Exhibit 2: Exfiltrated data types RedAlert noted on its dedicated leak site

<<< End >>>

Data indexing improves malicious usability

The emergence of vast quantities of leaked data enhances a BEC actor's ability to target an organization by strengthening the BEC attack chain while also undermining traditional defenses. ACTI assesses that the utility of dedicated leak site data has historically been limited by the difficulty of interacting with large quantities of poorly stored data. This has been cumbersome, time-consuming, and costly for actors, thereby creating a natural barrier for widespread abuse of the data, until now. ACTI found that several groups are making

their dedicated leak site data more accessible by moving away from Tor domains and toward publicly accessible sites. Moreover, sites like ALPHV and Industrial Spy offer searchable indexed data, including sensitive data such as employee personally identifiable information and financial data like that outlined in red in Exhibit 3. Because it facilitates and speeds access, this searchability is enormously beneficial to malicious actors seeking to weaponize data for secondary attacks.

Industrial Spy emerged as a data-selling marketplace in April 2022. It discloses some data freely and sells individual files for as little as one dollar. The operators actively organize and name folders with labels that reflect their content to make finding specific files easy. Folder 4 of Exhibit 3 (highlighted to showcase data indexing and obfuscated to protect potential victims) is an example of this.

<<< Start >>>

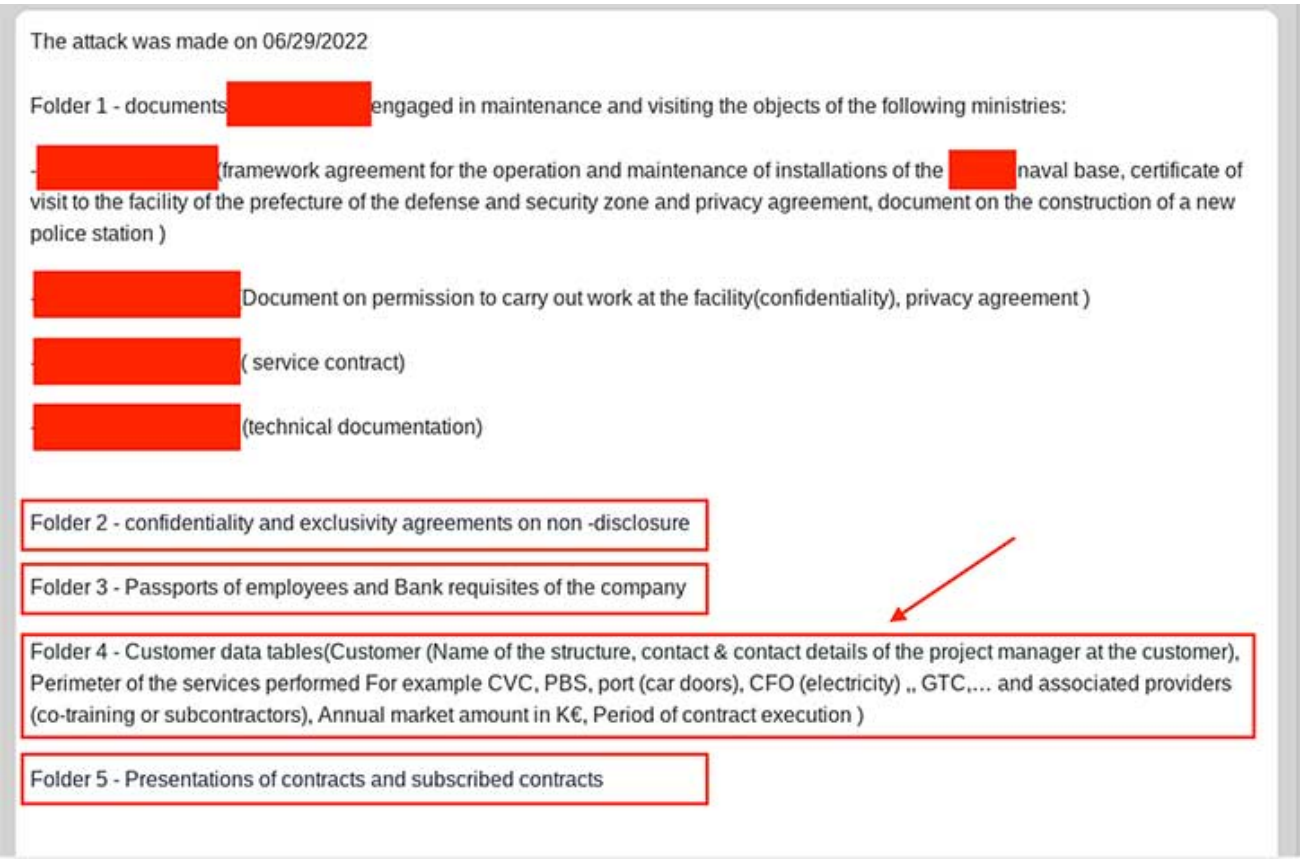


Exhibit 3: Sensitive data disclosed on the Industrial Spy marketplace

<<< End >>>

Moreover, the Industrial Spy marketplace now operates a working search function. ACTI tests found that threat actors can search for specific files such as employee data, invoices, scans, contracts, legal documents, email messages, and more. This search function also enables actors to hunt for data from specific industries and countries, for example, US-based engineering or insurance organizations.

Similarly, the ALPHV ransomware group has created an indexed and searchable database of its leaks (Exhibit 4, again obfuscated to protect potential victims), allowing anyone to search the ALPHV database for terms including employee names, contract data, invoices, leadership, and more. This facilitates locating data necessary to enrich a social engineering ploy. ACTI found "about 10,000" results when searching for "invoice" across indexed disclosures, as well as 6,000 results for "CFO," 10,000 for "accounting," and 10,000 for "email," showcasing the large amount of information available.

<<< Start >>>

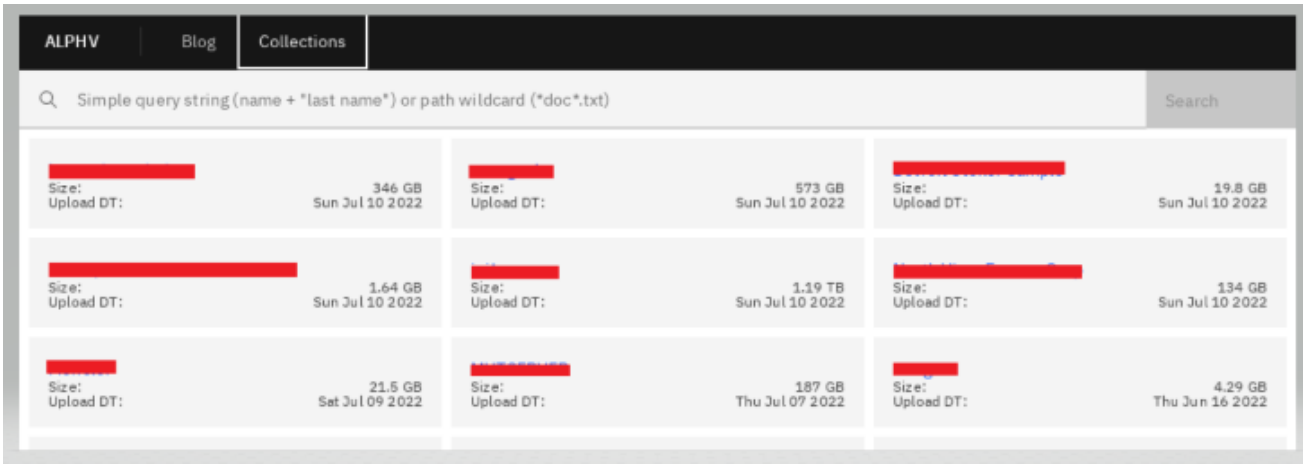


Exhibit 4: Indexed, searchable data hosted on ALPHV's dedicated leak site

<<< End >>>

ACTI assesses that the indexed and searchable databases like these help actors more efficiently acquire specific data versus downloading bulk data and hoping to find desired information.

Augmenting the BEC attack chain and defeating defenses

Although all types of cybercriminals can benefit from obtaining sensitive corporate data, it is especially helpful for those conducting attacks based on social engineering. ACTI assesses with high confidence that the availability of sensitive corporate data makes it increasingly difficult for employees of victim organizations to spot fake communications and avoid such attacks because actors can base their attacks on genuine documents from the victim organization. ACTI found that the most disclosed data types overlap with the data types most useful for conducting BEC and VEC attacks: financial, employee, and communication data, and operational documents (Exhibit 5). The “other” category includes marketing and training materials, etc. of less value to cybercriminals than the distinct data types above.

<<< Start >>>

Exhibit 5: Degree of overlap between available disclosed data and such data's usefulness for BEC and VEC attacks

<<< End >>>

ACTI assesses that the primary factor driving an increased threat of BEC and VEC attacks stemming from double-extortion leaks is the availability of data like that described above. This data is most useful during the reconnaissance and social engineering phases, particularly as the latter pertains to sending false invoices.

During the reconnaissance phase, malicious actors may study and weaponize the vast troves of sensitive internal company data, which provide rich sources of social engineering information. This includes insurance data, salary information, lease agreements, bank reconciliations, and more (highlighted in Exhibit 6).

<<< Start >>>

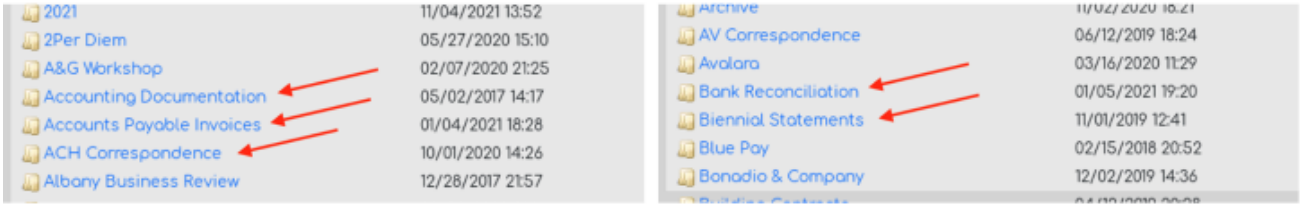


Exhibit 6: Internal data available on the Industrial Spy data extortion marketplace

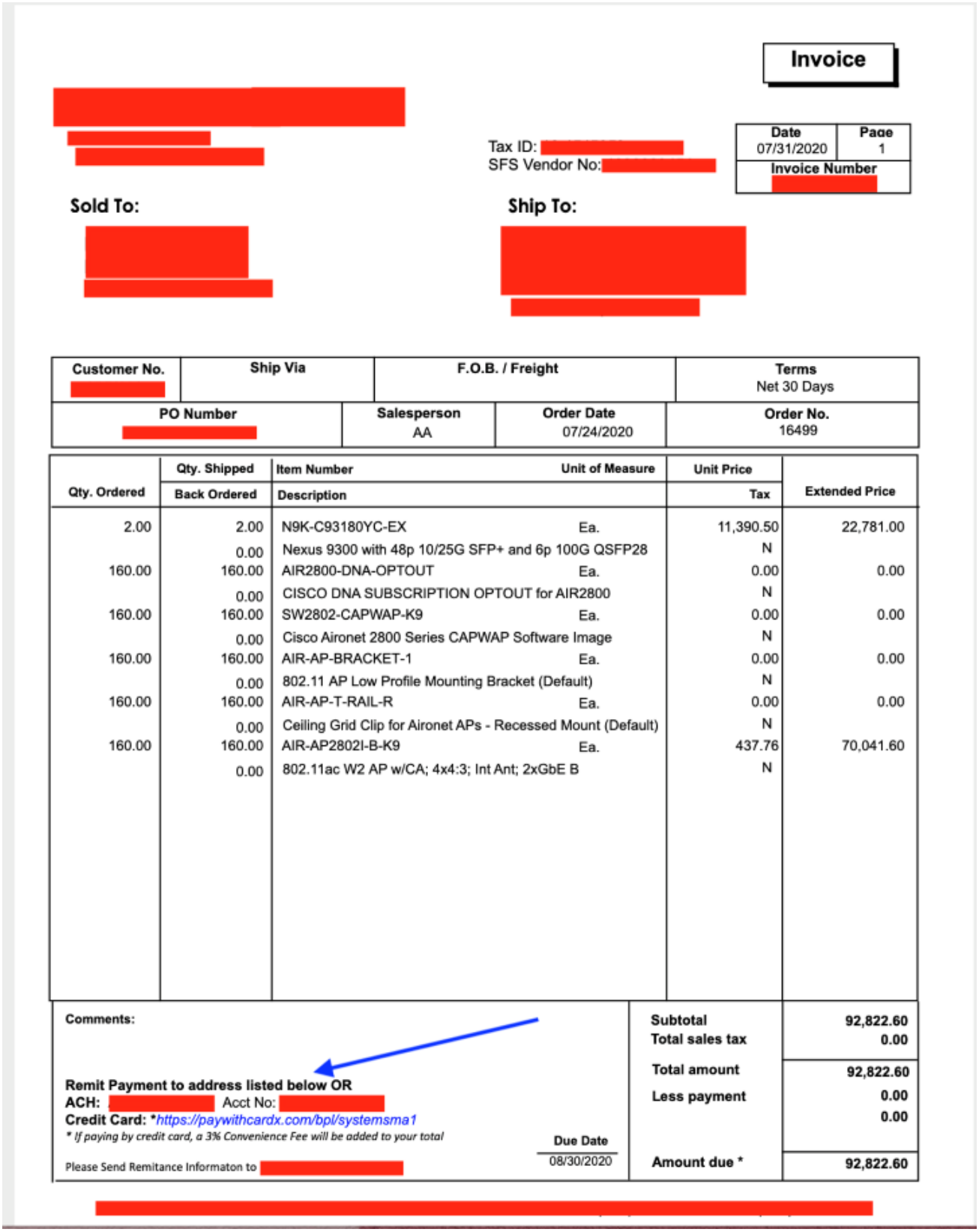
<<< End >>>

The social engineering phase is the most important and traditionally the most difficult part of a BEC attack and the phase that benefits most from dedicated leak site data. BEC attacks are inherently based on social engineering, with few technical roadblocks. This makes good social engineering the single most important determinant of a successful BEC attack. High-quality, well-crafted, and accurately scoped social engineering ploys give threat actors the ability to have higher success. Such data is a rich source of information about a victim company's day-to-day operations. A threat actor can increase the likelihood that a social engineering ploy will succeed by determining a target's internal language, such as company-specific acronyms and phrases, allowing threat actors to avoid use of non-standard company language, a tell-tale sign of fraud. Dedicated leak site data further reduces the likelihood of a target discovering a social engineering ploy by allowing actors to better adhere to internal organizational pathways. For example, it facilitates following typical, anticipated communication channels and command chains.

Finally, malicious actors can use this data to improve the timing of an attack. Actors can initiate a social engineering ploy when the targeted individual and organization are most vulnerable, such as during acquisitions or vendor contract renewals, while traveling, or when other information is available only through insider knowledge. For VEC attacks, these effects are even more powerful, given the large amounts of sensitive dumped data that is normally shared only between a primary target and its vendors. Specifically, contractual data, invoices, financial agreements, payment schedules, orders, and purchase histories are all abundantly available on dedicated leak sites, enabling actors to mimic a vendor more closely than they could otherwise.

The final step of a BEC or VEC attack often involves sending a fraudulent invoice to a victim or a victim's supplier. Dedicated leak site data often includes genuine invoices that actors can easily alter for use in an attack. Exhibit 7 shows a genuine invoice ACTI found on the Industrial Spy data extortion site, obfuscated to protect potential victims. After carrying out a well-crafted social engineering campaign, an actor could change such an invoice's accounting details (marked with a blue arrow) to an actor-controlled account and send the modified invoice to the target.

<<< Start >>>



Invoice

[redacted]

Tax ID: [redacted]
SFS Vendor No: [redacted]

Date	Page
07/31/2020	1
Invoice Number	[redacted]

Sold To:

[redacted]

Ship To:

[redacted]

Customer No.	Ship Via	F.O.B. / Freight	Terms
[redacted]			Net 30 Days

PO Number	Salesperson	Order Date	Order No.
[redacted]	AA	07/24/2020	16499

Qty. Ordered	Qty. Shipped / Back Ordered	Item Number / Description	Unit of Measure	Unit Price / Tax	Extended Price
2.00	2.00	N9K-C93180YC-EX	Ea.	11,390.50	22,781.00
	0.00	Nexus 9300 with 48p 10/25G SFP+ and 6p 100G QSFP28		N	
160.00	160.00	AIR2800-DNA-OPTOUT	Ea.	0.00	0.00
	0.00	CISCO DNA SUBSCRIPTION OPTOUT for AIR2800		N	
160.00	160.00	SW2802-CAPWAP-K9	Ea.	0.00	0.00
	0.00	Cisco Aironet 2800 Series CAPWAP Software Image		N	
160.00	160.00	AIR-AP-BRACKET-1	Ea.	0.00	0.00
	0.00	802.11 AP Low Profile Mounting Bracket (Default)		N	
160.00	160.00	AIR-AP-T-RAIL-R	Ea.	0.00	0.00
	0.00	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)		N	
160.00	160.00	AIR-AP2802I-B-K9	Ea.	437.76	70,041.60
	0.00	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE B		N	

Comments:

Remit Payment to address listed below OR
ACH: [redacted] Acct No: [redacted]
Credit Card: *https://paywithcardx.com/bpl/systemsma1
** If paying by credit card, a 3% Convenience Fee will be added to your total*

Please Send Remitance Informaton to [redacted]

Due Date 08/30/2020

Subtotal	**92,822.60**
Total sales tax	**0.00**
Total amount	**92,822.60**
Less payment	**0.00**
	0.00
Amount due *	**92,822.60**

[redacted]

Exhibit 7: Genuine invoice that ACTI discovered on a dedicated leak site

<<< End >>>

ACTI found similar invoices in nearly all dumps across various dedicated leak sites. In addition, an ACTI search for invoices in July 2022 rendered more than 10,000 hits on two leak sites alone, showcasing the vast volumes of data available.

Beyond enabling a threat actor to conduct a more sophisticated attack, this type of data circumvents traditional socialengineering attack defenses.

Conclusion

The widespread disclosure of data as part of ransomware attacks has flooded the criminal underground with sensitive data from corporate networks that practically anyone can view and obtain. The availability of the data has synergetic effects. First, operators can leverage the data to augment and enrich entire BEC and VEC attack chains. Second, the data can circumvent defenses that the industry has been promoting to protect against attacks based on social engineering.

The availability of internal data also increases the risk of secondary attacks driven by but unrelated to initial ransomware events. Such risk extends beyond a primary ransomware attack victim to other organizations that do business with the victim or who operate within the victim's supply chain.

Mitigations

To prevent BEC attacks, ACTI suggests that businesses and consumers:

- Remain skeptical of changes in payment plans, even from genuine invoices and trusted vendors or suppliers.
- Validate invoice amounts through a communication medium that differs from the one through which an invoice was received.
- Remain extra vigilant against new invoices or communications regarding payments after a data exfiltration event, whether that event occurred at one's own company or at a company within the same supply chain.

To prevent and mitigate socialengineering attacks, ACTI suggests that businesses and consumers:

- Check the source of each email and ensure email senders are genuine.
- Look up phone numbers to determine their legitimacy before returning unforeseen calls and avoid providing sensitive data to unknown callers.
- Locate official website URLs rather than clicking on links within messages.
- Use multi-factor authentication to prevent or delay the success of an attack in which actors access passwords through social engineering.
- Continuously monitor critical systems.
- Identify and protect critical assets.
- Regularly check SSL certificates.

- Maintain a closed and controlled digital footprint; oversharing of personal details online through social media offers criminals more information to work with.
- Train employees to limit the amount of work information they share on social media platforms and how to identify social engineering ploys.

To prevent and mitigate data extortion attacks, ACTI suggests that businesses and consumers:

> Limit or avoid the exposure of internal corporate technical procedures and infrastructure in presentations from third-party technology partners.

Accenture Security *is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us @AccentureSecure on Twitter, LinkedIn or visit us at accenture.com/security.*

Accenture Cyber Threat Intelligence

Subscription Center

Subscribe to Security Blog Subscribe to Security Blog

Subscribe