accenture

Global Incident Report: Deep Web Database and Network Access Sales Affecting Russia Ukraine Dispute

Scenario

Deep web threat actors are posting advertisements for assets, including databases and breached networks, that could interest buyers involved in the ongoing Russia Ukraine conflict. Since mid-January 2022, Accenture Cyber Threat Intelligence (ACTI) has identified deep web actors advertising databases and network accesses containing information on Russian and Ukrainian entities. If genuine, well-placed adversaries could potentially cripple affected organizations.

Discovery Date

January-February 2022

Related Forums and Marketplaces

- RaidForums
- Free Civilian .onion site

Involved Threat Actors or Groups

- vlakyla
- GodLevel
- an3key
- Free Civilian

Evaluation

As of Feb. 11, 2022, ACTI assesses it is likely that as intelligence warnings and postings related to Russia and Ukraine increase, deep web actors will continue to increase their offerings for databases and network accesses relevant to the Russia Ukraine conflict in hopes of gaining high profits. Global events occasionally serve as motivating factors for

malicious actors to claim they are selling important and relevant data for profit, regardless of whether such data is genuine or even exists.

WhisperGate

The WhisperGate destructive malware attacks targeting Ukraine government, non-profit, and IT organizations from Jan. 13-14, 2022[1] may inspire deep web actors to increase network access sales for organizations with critical assets in Russia or Ukraine. Such accesses could enable prospective buyers to conduct similar types of campaigns within Russia or Ukraine or even against other nation-states involved in the dispute, such as the United States or those in Europe. Nation-state actors could purchase and leverage network accesses to critical infrastructure organizations, such as telecommunications or energy organizations, as well as banks. They could use the accesses with asymmetrical tactics to cause disruptions, including depriving users of interconnectivity, energy, or financial transactions, if timed correctly.

In the days and weeks following the WhisperGate attacks, ACTI has observed several instances of threat actors and groups advertising databases allegedly containing the personally identifiable information (PII) of Ukrainian citizens, as well as breached network accesses, on underground sites such as RaidForums and .onion sites. The following provides examples of this type of activity.

GodLevel

On Feb. 2 2022, RaidForums user "GodLevel" advertised access to a subdomain belonging to an identified Ukrainian agricultural exchange. GodLevel indicated that they have shell and database access to the subdomain, which would enable a user to modify databases and have schema and access privileges. Additionally, GodLevel provided a screenshot indicating they can access payment information and contracts. According to the victim exchange's official website, the victim organization is responsible for organization exchange trades, commodity derivatives, mortgages, mortgage certificates, creating settlement and clearing systems for servicing concluded exchanges, and setting market prices for agricultural products. As of Feb. 10, 2022, GodLevel is selling this access for approximately $US160.

An attacker could potentially use compromised system access to elevate user privileges and make use of associated domains to obtain PII and payment card data, resell exfiltrated data, deploy malicious software such as ransomware, deface websites on the affected subdomain, or possibly even disrupt active exchanges and trades. The asking price for subdomain access is relatively low, suggesting GodLevel previously had trouble selling access and subsequently reduced the price, or that the actor may not realize the damage an attacker could inflict with the purchase.

Free Civilian

Since late January 2022, actors on several underground sites have shared links to a Tor .onion website called "Free Civilian" (Exhibit 1). The site claims to sell Ukrainian citizens' personal data from several Ukrainian government sites, including agencies involved in

[1] https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

building and housing, law enforcement, and the issuance of digital documents. As of Feb. 10, 2022, the Free Civilian site indicates it has sold two of five databases and that three are still available for purchase. The databases are noted as “gov.ua ” databases, are 3.3-765 GB in size, and have no listed prices. The site operator(s) have instructed prospective buyers to contact them via the TOX messaging platform and indicated they are willing to conduct transactions through a third party, which actors typically do to reduce the risk of scams.

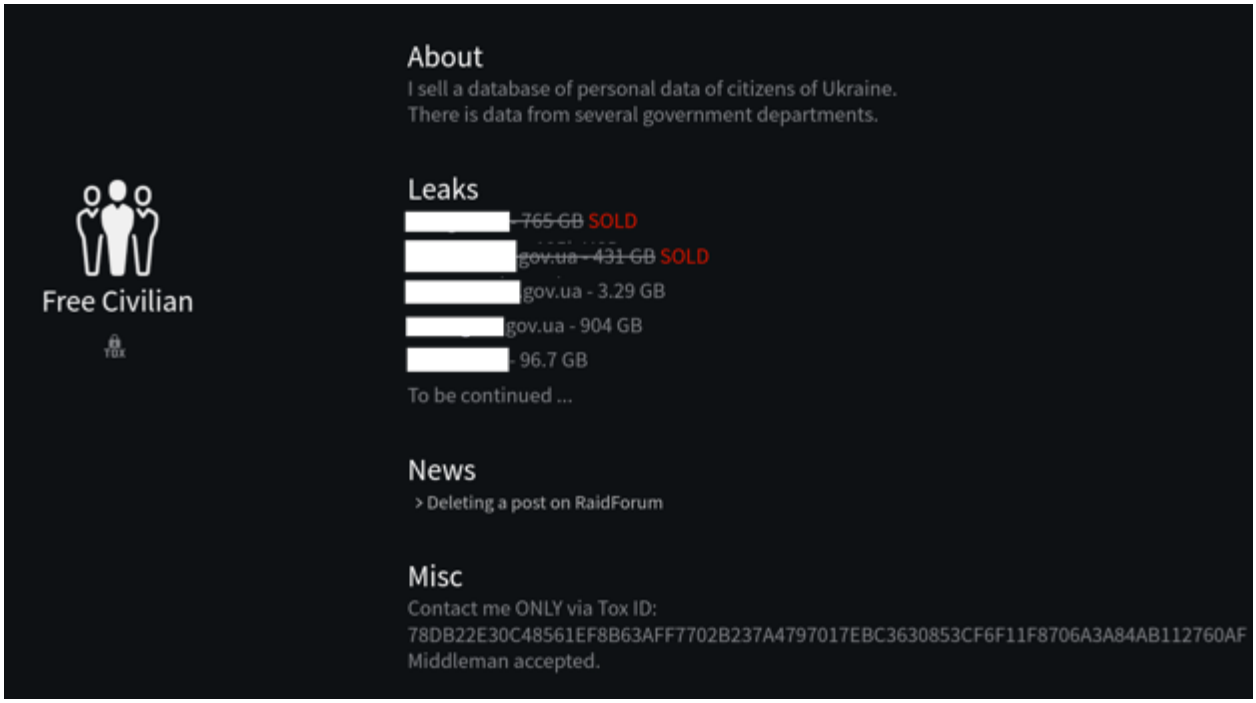

Exhibit 1: Free Civilian Website Advertising Ukrainian Government Data in February 2022

an3key

On Jan. 27, 2022, RaidForums user “an3key” shared a SQL database allegedly from a Ukrainian federal agency. According to an3key, the database contains information on wanted criminals, including names, birth dates, photos, criminal histories, and more. The user indicated the data is from 2021 and provided two links for users to download the data; however, at least one forum user has suggested an3key did not obtain the criminal information through a breach, as the data is publicly accessible via a Ukrainian government website.

A malicious actor could potentially use the data in the database to harass affected individuals through tactics such as extortion; or, depending on the full scope of data available, an attacker could potentially commit identity theft. Malicious actors could also leak the data on other underground forums and increase the likelihood of future harassment or identity theft.

RaidForums User

On Jan. 23, 2022, a RaidForums user advertised the sale of network access to a Ukrainian bank and power plant, including administrator accounts. The user claimed to know the location of vulnerabilities in the systems, which the user also offered for sale.

The user in question advertised access to an identified Ukrainian bank, including alleged access to more than 70 administrator accounts, and the location of the vulnerability in the bank's networks that allowed the collection of bank data. The user claims an attacker can use the accesses to gain entry to the vulnerable host's administrator panel. Additionally, the user advertised 220 email addresses and the location of a vulnerability in a system associated with a large private investor in the Ukrainian energy industry; however, the user did not identify the email addresses or the level of access that exploitation of that vulnerability would provide. The user also did not specify prices for access to either network, though they indicated prices are negotiable.

As of early February 2022, this user has accumulated numerous positive reputation points on RaidForums by conducting successful transactions with site members. In other RaidForums advertisements, the user has claimed to have discovered SQL injection vulnerabilities in the networks of biotechnology companies allegedly involved in developing COVID-19 vaccines, as well as U.K. telecommunications organizations and U.S. banks. If the advertised accesses are genuine, an adversary could potentially disrupt financial transactions and energy supplies in Ukraine. Given the ongoing Russia-Ukraine conflict, ACTI assesses it is probable the user will garner high prices for this offering.

vlakyla

On Jan. 22 2022, RaidForums user "vlakyla" posted an advertisement for the sale of Ukrainian citizens' PII, including names, phone numbers, and email addresses (Exhibit 2). While it is unclear how many citizens are on this PII list, vlakyla provided a link to download a small portion of the data to prove its legitimacy. vlakyla did not specify a price for the full data set; however, the actor instructed prospective buyers to contact them through the RaidForums private messaging system, so they may be providing it to buyers individually. The actor has minimal feedback on the forum, making it difficult for ACTI to accurately assess the credibility of the actor or the data as of Feb. 11, 2022.

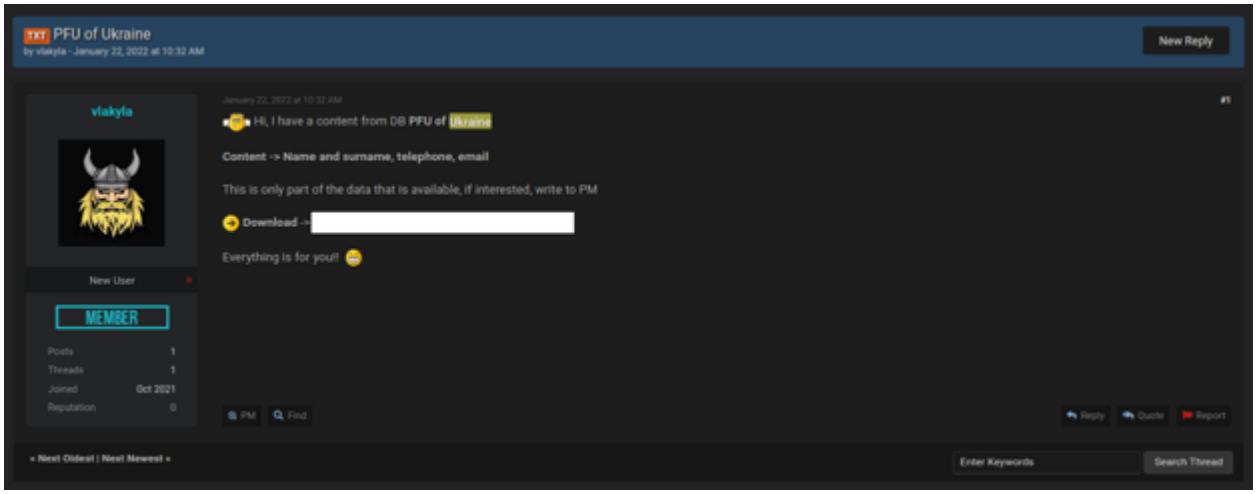

Exhibit 2: Actor vlakyla Advertising Ukrainian Citizens' PII on RaidForums on Jan. 22, 2022

An attacker could potentially use the Ukrainian citizen PII to conduct social engineering, phishing, or smishing attacks; additionally, if the data includes passwords, an attacker could use it to perform credential-stuffing attacks or account takeover (ATO) fraud. vlakyla's customers could also subsequently resell the data to other malicious actors, further increasing the likelihood of malicious activity targeting those individuals with PII in the dataset for sale.

Mitigation

To mitigate unauthorized network access, ACTI suggests:

- Being aware that seemingly criminal activity might be masking or enabling politically motivated activity.
- Maintaining best practices such as patching, firewalling infection vectors, updating anti-virus software, enforcing an off-site backup policy, practicing how to restore from backups, and using application allowlists.
- Securing Remote Desktop Protocol (RDP) connections with complex passwords, virtual private networks, and network-level authentication, if RDP connections are necessary.
- Scanning networks for machines using RDP and disabling the protocol if not needed.
- Checking for the presence of unauthorized remote access utilities, such as LogMeIn or TeamViewer, on internal networks.
- Monitoring for large amounts of suspicious outbound traffic and other abnormalities in network traffic flow that might indicate unauthorized remote sessions.
- Restricting login attempts and deploying multi-factor authentication where possible.
- Ensuring third-party vendors follow strict security policies, especially those pertaining to remote network access.

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 674,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at accenture.com.

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, part of Accenture Security, has been creating relevant, timely and actionable threat intelligence for more than 20 years. Our cyber threat intelligence and incident response team is continually investigating numerous cases of financially motivated targeting and suspected cyber espionage. We have over 150 dedicated intelligence professionals spanning 11 countries, including those with backgrounds in the intelligence community and law enforcement. Accenture analysts are subject matter experts in malware reverse engineering, vulnerability analysis, threat actor reconnaissance and geopolitical threats.