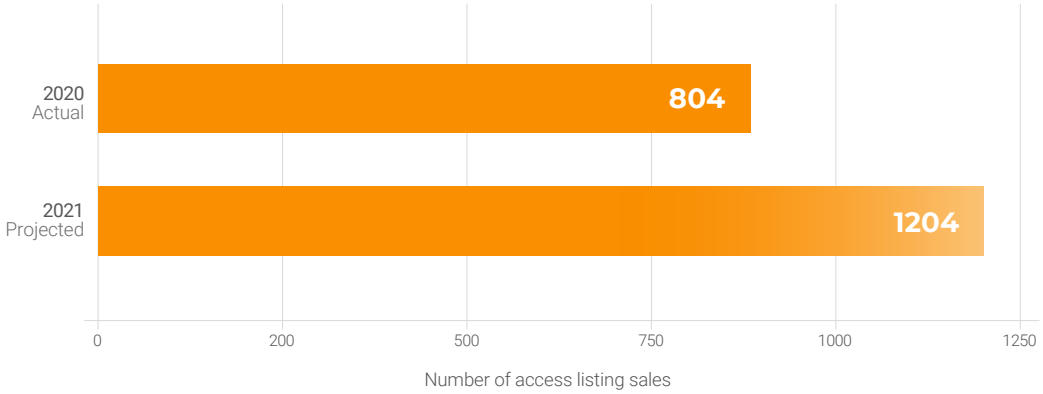
Flashcard Report: **Monetization of Cybercrime**

Credential Market Activity Is Increasing

Activity on dark web marketplaces that trade access to compromised networks has increased dramatically (see graph below). This business has evolved to include items that were rare in these markets a few years ago as they used to be primarily focused on selling stolen credit card data.



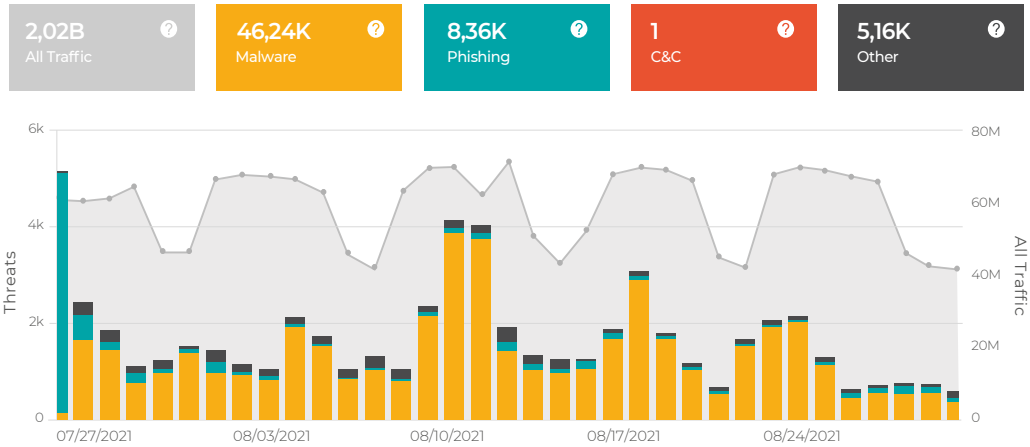
Access listings sales
2020 - 2021

Source:
All Access Pass: Five Trends with Initial Access Brokers, ke-la.com (2020 figures extrapolated from H2 2020, 2021 figures extrapolated from H1 2021).

Stolen credit card data provided a direct path to monetization. We've seen an acceleration of monetization of any type of cybercrime activity, particularly of those items and data that aren't as easily monetized as credit card details.

Explaining the Surge in Demand

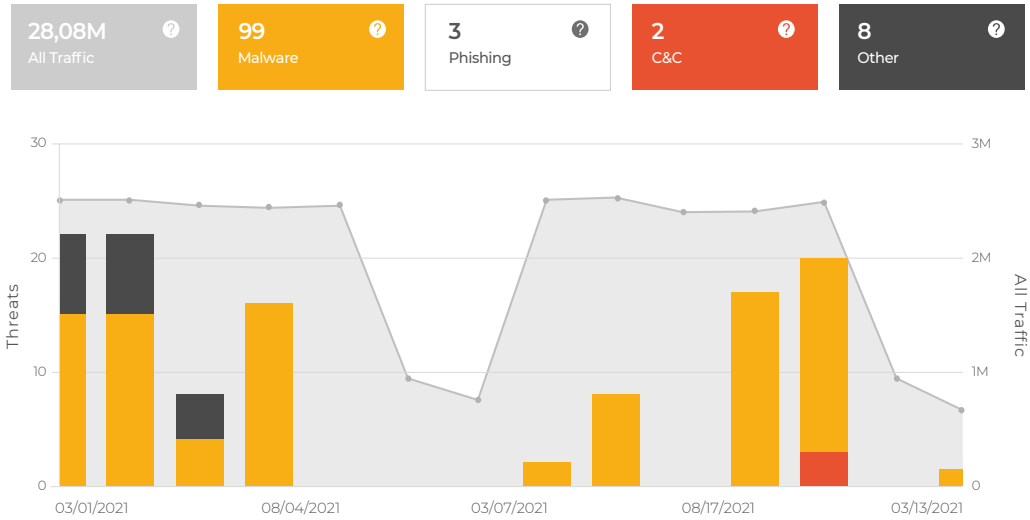
When you analyze the traces of adversarial contact observed in networks that have been compromised with ransomware, you can see the source of the demand that drives the acceleration observed in dark web marketplaces.



In this image from the Lumu Portal, a phishing attack led to the installation of a cryptojacking botnet (dark gray), malware (yellow), and eventually a solitary C&C contact (red, not visible at this scale).

The image shows that long before a ransomware incident materializes, networks of compromised organizations exhibit an exacerbated number of contacts with other types of incidents that are rarely associated with ransomware like phishing, crypto mining botnets, and spam botnets.

Modern ransomware incidents require time to compromise as many assets as possible, disrupt operations as much as possible, exfiltrate as much data as possible, and exert maximum pressure through extortion. This time varies from as little as 1 month to well over six months.

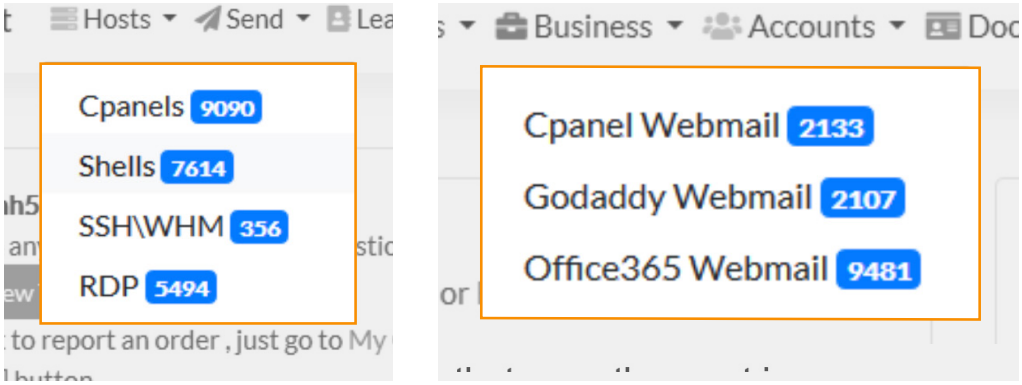


This image from the Lumu Portal shows how an attack that initially started with cryptojacking (dark gray) and malware (yellow) led to a C&C contact (red) with REvil/Sodinokibi ransomware infrastructure.

However, while the ransomware attack is maturing, criminals are extracting every possible cent from the compromised organization. For example, it's common to see the mining of digital currencies in the network, reselling the compromised infrastructure, and using it to launch spam campaigns that will compromise future targets of the same scheme. In this way, various types of access to these compromised networks end up on dark web markets.

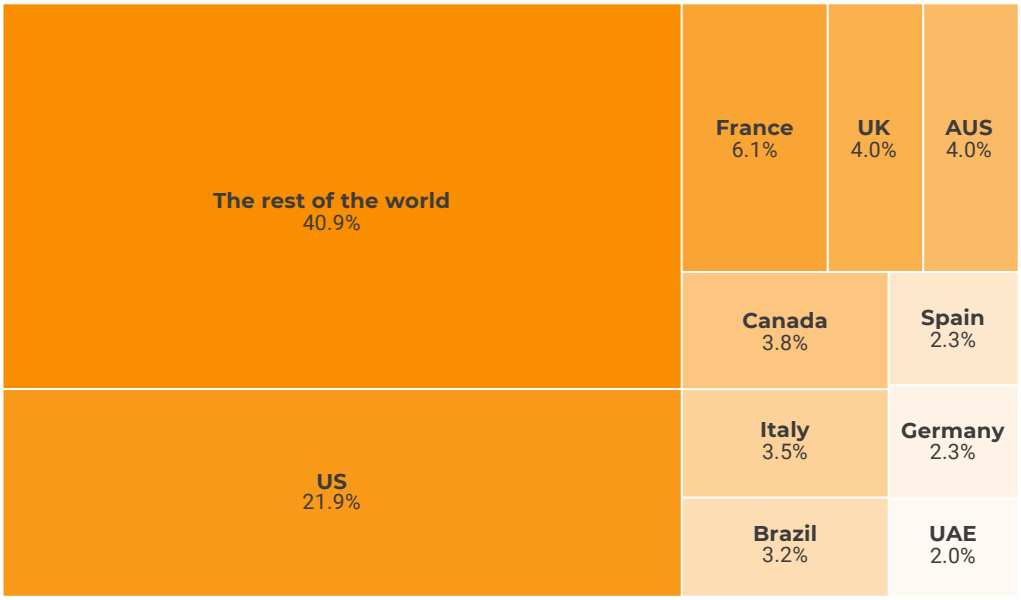
Where There's a Will, There's a Way

As you can see above, a ransomware attack is hardly ever an isolated event. The attack usually starts with a 'lesser' compromise, which is easily launched through the access offered by online credential markets.



Screenshot from a dark web forum where access to various types of initial access to compromised networks is available for sale.

These markets offer access to everything from web hosting panels and webmail servers to remote desktop access. The compromised organizations represent every nation, industry, and size.



Network access victims' location, TOP - 10

1000+ access listing analyzed

Source: All Access Pass: Five Trends with Initial Access Brokers, ke-la.com

Credentials Offer Easy Access to the Network

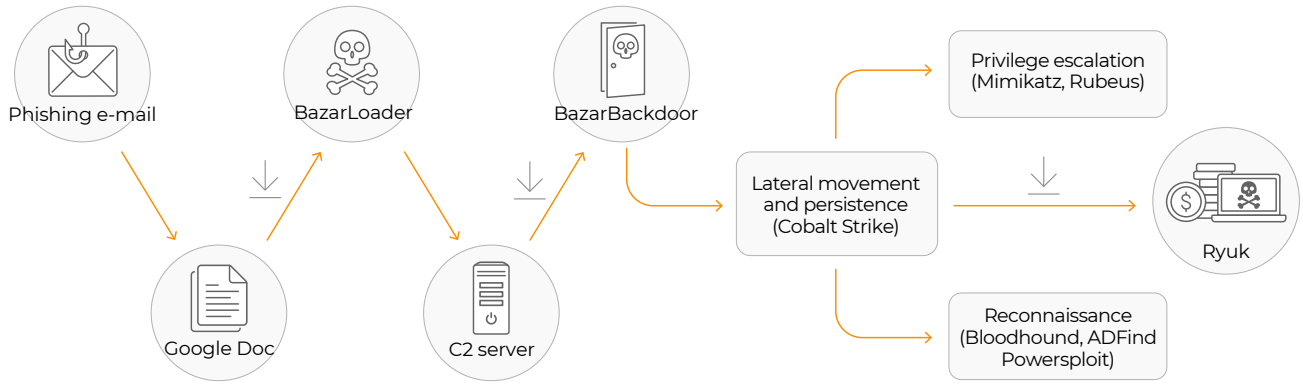
Access to Remote Desktop Protocols (RDP) in particular can signify that the threat actor has control over your network. RDP access allows attacks to evade detection through VPNs or SDPs, such as in the case of the Florida water treatment where attackers were able to alter water acidity to dangerous levels. This and other access types establish the perfect springboard from which to move laterally across your entire network.

Monetization Techniques Vary

There are many ways for threat actors to make money from your network. These include:

- Crypto Mining Botnets
- Spam Botnets
- Adware installs
- Drop/Deploy Other Malware
- Selling backdoor access to the network
- Exfiltrating Sensitive Data
- Exfiltrating Credit Card Credentials
- Blackmail
- Ransomware

Attacks Evolve Using Different Techniques



Ranomware-as-a-service is a well-established business model where ransomware can be bought at minimal cost and requiring minimal skills. Starting from April 2019, threat actors started using traditional malware to gain a foothold in a company that they could sell to ransomware specialists, in a tactic called malware-delivery-as-a-service. This has led to the emergence of 'ransomware chains' where the ransomware is preceded by an associated malware type.

Some ransomware chains include:

- Emotet → TrickBot → Ryuk
- IcedID → REvil / Sodinokibi
- Qakbot → Egregor
- Zloader → DarkSide

There Are No 'Minor' Threats

The easiest and fastest way to monetize access to the network is through botnets. Therefore, this is usually the first type of compromise seen on the network. The cybercriminal will always look for the lowest resistance, lowest cost, and highest-impact path for perpetuating their attacks. The attack will escalate when the attacker has enough resources, time, and proof that the ransomware attack is worth their time. Ransomware attacks take as little as 3 days to mature from the initial compromise.

We encourage organizations to treat all compromises as evidence of a serious ongoing attack.
Open a Lumu Free account to know your real-time exposure and level of compromise.