



ZEROFOX[®]

Your Intelligence Digest

**It's a Digital World.
Engage Securely.**

New RaaS Project Dubbed 'Mallox' Announced

Untested threat actor "Mallx" announced a new ransomware-as-a-service (RaaS) project, dubbed "Mallox," on the Russian language Dark Web forum "RAMP." The actor said they would prefer to work with affiliates who have already established initial network access to companies. Features of the RaaS project include:

- Written in C++
- Controlled via web panel
- Chat functionality to negotiate with victims
- Leverages strong encryption (ECC and ChaCha20)

The actor offered to split any successful ransom payments 80-20 in their favor, which is typical of most RaaS projects.

ZeroFox researchers assess the number of ransomware attacks will likely increase continue to grow in 2023, since the arrival of new RaaS projects, like "Mallox", emerged on the criminal underground, just weeks into the new year.

Original post from threat actor "Mallox" announcing a new ransomware-as-a-service (RaaS) project dubbed "Mallox"

New RaaS Project Dubbed 'Mallox' Announced (Cont.)



Mallox

Nov 12, 2022

Messages	1
Reaction score	0
Points	1

Saturday at 10:39 PM

Криптолокер Mallox ищет пентестеров в команду

Если у вас есть собственный материал, то мы готовы предложить качественный софт и поддержку

Особенности:

- Чистый C++ код
- Веб-панель с регулировкой цен для клиентов и чатами
- Шифрование эллиптические кривые + чача20

Условия:

80/20

Неактивных будем со временем отключать

Service Develops Custom Cyber-Attack Infrastructure

New and untested threat actor “XORacle” advertised a new service that develops custom cyber-attack infrastructure on the English language Dark Web forum “CryptBB” and the predominantly Russian language Deep Web forums “XSS” and “Exploit.” This is significant because the service would likely lower the barrier to entry for most threat actors, allowing individuals of any skill level to launch more sophisticated attacks, if they can afford it. The actor said they can program multiple tools, including:

- Custom malware
- Command and control (C2) panels
- Phishing pages
- Automated scripts
- Malicious web browser extensions
- Exploits for unpatched vulnerabilities

ZeroFox researchers assess the actor is likely legitimate because several peers have already vouched for the service, noting the actor’s professionalism and their below-market pricing. Additionally, the actor agreed to use an escrow service, which would require them to utilize a forum administrator or middleman to complete any transactions.



Original post from threat actor "XORacle" advertising a new service that develops custom cyber-attack infrastructure

Service Develops Custom Cyber-Attack Infrastructure (Cont.)



XORacle •
Newbie
Member

Posts: 1
Joined: Jan 2023
Reputation: 0

#1

01-18-2023, 12:52 PM

Hello, CryptBB!

We are an army of two engineers with years of experience in developing sophisticated security software. Our main stack is Rust/Golang/Python for backend and, as usual, HTML/CSS/Javascript for frontend (with popular frameworks, such as: Angular, Vue, React). We developed/analyzed a plethora of cross-platform malware strains during our career, such as: RATs, Stealers, Clippers, Keyloggers, Rootkits, Lockers, Cloaks, C2 Panels, Browser Extensions, etc.

Take a look at our brief offering below, which can be customized for each customer:

- * Custom malware development
- * Desktop application development
- * Custom website/webapp development
- * Command and Control panels
- * Website cloning
- * Phishing pages
- * Scripts
- * Bots
- * Browser extensions
- * Automated project deployment
- * Integration with third-party APIs
- * And much more!

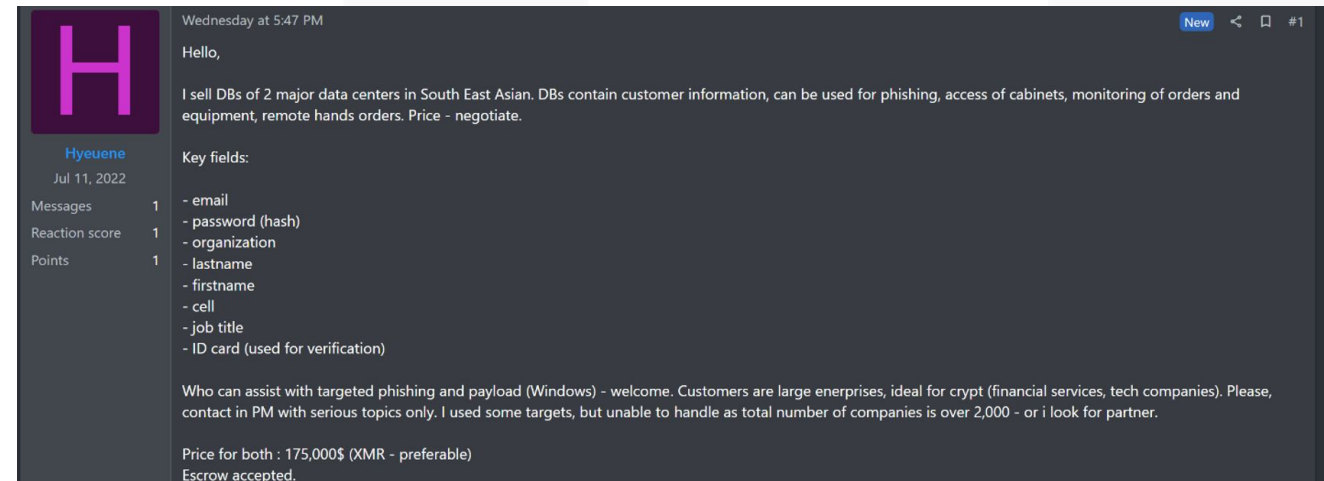
Alleged Data Breaches Impact Various Tech & Financial Services Companies

Untested threat actor “Hyeuene” announced data breaches impacting two large data centers in Southeast Asia on the Russian language Dark Web forum “RAMP.” The alleged datasets contain the personally identifiable information (PII) of more than 2,000 employees from multiple high-profile, undisclosed tech and financial services companies. This is significant because a threat actor can likely use this information to launch spear-phishing attacks or malware campaigns against the target organizations.

Compromised data includes:

- Full names
- Phone numbers
- Email addresses
- Hashed passwords
- Employers
- Job titles
- ID card numbers

The actor charged \$175,000 USD for the complete datasets.



Automated Telegram Service Offers Botnet Logs For Various Domains

Untested threat actor “omegarequest” advertised a new automated Telegram service, dubbed “Omega BOT REQUEST,” that offers public and private botnet logs for various domains on the predominantly Russian language Deep Web forum “Exploit.” The bot allows threat actors to query a database containing more than 759 million sets of compromised account credentials for different services. After purchase, the bot deletes these records from the database, preventing the resale of credentials. This is notable because most automated botnet log shops on Telegram and similar platforms typically resell email and password combinations from public botnet logs for a limited number of domains, often making it more difficult for threat actors to successfully compromise target accounts.

There was a flat fee of \$25 USD for the service. The actor charged an additional \$0.01 to \$0.25 per set of credentials, depending on the order quantity.


Request BOT - your request from my base [URL:LOGIN:PASS]
 By omegarequest, 5 hours ago in [Finance] - billing, banks, accounts, logs

omegarequest
 byte

 Paid registration
 1 post
 Joined
 01/30/23 (ID: 142136)
 Activity
 дрыго / other

Posted 5 hours ago

[YOUR REQUEST FROM LOGS]
 It will suit those people who have their own request . Also for those people whose request requires unique logins or a phone number.
 Now I will explain in more detail
TOTAL : 759 816 313 Lines [FROM PRIVATE-PUBLIC LOGS]
 1 LINES contains all user information, sites he visited and authorization data from these sites
 You tell us your request
 PRICE starting with 25+\$ and after
 IF REQUEST HAVE TOTAL
 1-100 LINES - 0.25\$ per 1 lines
 100-1000 lines - 0.051\$ per lines
 1000-10000 - 0.018\$ per lines
 10000+ - 0.005\$ per lines