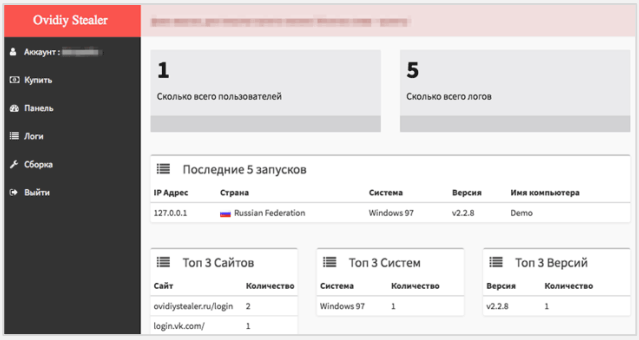
Cybercrime as a Service

Definition

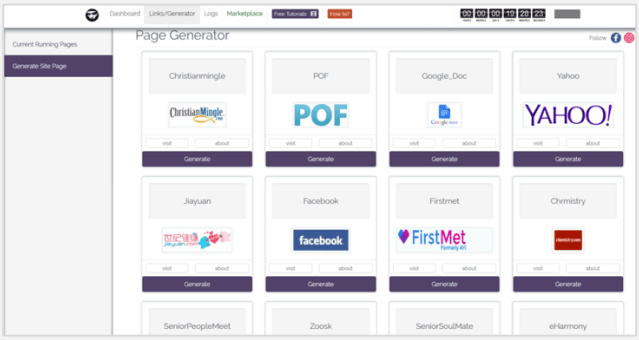
Cybercrime-as-a-Service (CaaS) is a criminal application of the ‘as-a-service’ model currently revolutionising legitimate business models.

For criminals, CaaS offers access to all manner of digital resources needed to commit cybercrimes, such as malicious software (malware), botnets (networks of computers infected with malware), hacking specialists, databases of stolen personal information, penetration testing of potential targets, open-source research, and much more. As in the legitimate business world, CaaS facilitates specialisation by providers; leading to improved quality due to competition, increased market penetration through resellers, and a reduction in resources and skills barriers to entry for aspiring cybercriminals.

Ovidiy Stealer malware steals passwords and is marketed on Russian-language websites.



Hackshit is a Phishing-as-a-Service (PhaaS) platform that offers low cost ‘automated solution for the beginner scammers’.



Source: KnowBe4 blog (2017)

The web of cybercrime

In November 2016, the Avalanche network was taken down by a coalition of law enforcement agencies from 30 countries, after more than four years of work. Avalanche is responsible for victimizing more than 500,000 people in 40 countries, and conservative estimates of financial losses total in the hundreds of millions of dollars. In total, 39 servers were seized, 221 more were sink-holed (permanently disabled), and 5 people were arrested. How could five people be responsible for so much damage and avoid arrest for more than 7 years? The answer is CaaS.

What services are available through CaaS?

Research-as-a-service

- Legal or illegal collection of information on victims
- Resale of stolen personal data or email addresses
- Identification and sale of ‘zero-day’ vulnerabilities

Infrastructure-as-a-service

- Hosting of malware on secure networks
- Rental of established botnets for Distributed Denial-of-Services
- Cloud-based computing power for operations

Crimeware-as-a-service

- Sophisticated exploits and other malware for rent
- Design and delivery of customized solutions
- Rapid adaptation to defeat cybersecurity defences
- Development of malware for niche markets

Hacking-as-a-service

- Outsourcing of a complete cyber-enabled attack
- Technical support for cybercrime activities
- Robust and dynamic integration of stolen data
- Minimal technical expertise required by customer

While these categories cover the most common CaaS offerings, services provided can range from penetration testing of anti-virus software to disabling of home security systems and much more. As more of our devices become ‘smarter’ and connected to the internet, those too can become vulnerable to criminals through CaaS.

How is Standard Chartered Bank facing the threat of Cybercrime?

An integrated approach to cybercrime

Standard Chartered Bank (SCB) has created a dedicated Cyber-Enabled Financial Intelligence ("CyFI") Group to focus on identifying, analysing, mitigating and reporting cyber-enabled financial crime. This team is producing intelligence via fusion of financial data, cyber threat intelligence, web research, mining of restricted access sites, and much more. Working in collaboration with other internal SCB teams, industry partners and law enforcement, CyFI is focused on proactively identifying, mitigating and preventing cyber-enabled financial crime risks to the Bank through early warnings, improved awareness, and actionable inputs for financial crime and cybersecurity controls.

Industry and law enforcement collaboration

SCB is engaging with industry and law enforcement stakeholders through organizations such as the National Crime Forensic Training Alliance (NCFTA). By embedding an analyst in the New York City NCFTA office, the Bank is well-positioned to participate in joint projects to identify new technologies and methods of proactively identifying and disrupting cyber-enabled financial crime. Another example of SCB's outreach is membership in the Financial Services – Information Sharing and Analysis Center (FS-ISAC), a cyber threat intelligence clearinghouse providing rapid dissemination of cyber threat intelligence. Involvement with these organizations is a critical element of maintaining a tactical and strategic advantage over cyber-enabled criminal networks.

Regulators focus on cyber-enabled financial crime

"The proliferation of cyber-enabled financial crime is not lost on regulators seeking to protect the financial systems. In October 2016, FinCEN (The Financial Crimes Enforcement Network) issued new guidance on how Bank Secrecy Act (BSA) regulations apply to cyber events, cyber-enabled crime, and cyber-related information.

The advisory provides guidance with respect to:

1. Suspicious Activity Reports (SARs) in connection with cyber-enabled crime and cyber events;
2. Including relevant cyber-related information in SARs;
3. Encouraging collaboration between in-house cybersecurity units and AML units; and
4. Sharing cyber-related information among financial institutions to combat money laundering, terrorism financing, and cyber-enabled crime.

Financial institutions will face expanded BSA reporting requirements under the recently enacted New York State Department of Financial Services (DFS) cybersecurity regulations, which came into effect March 1, 2017, including an expanded definition of cyber events triggering BSA reporting. Financial institutions should consider how the convergence of cyber security and financial crimes compliance impact its target operating models to ensure seamless coverage."

Patricia Sullivan | Regional Head, Financial Crime Compliance Americas