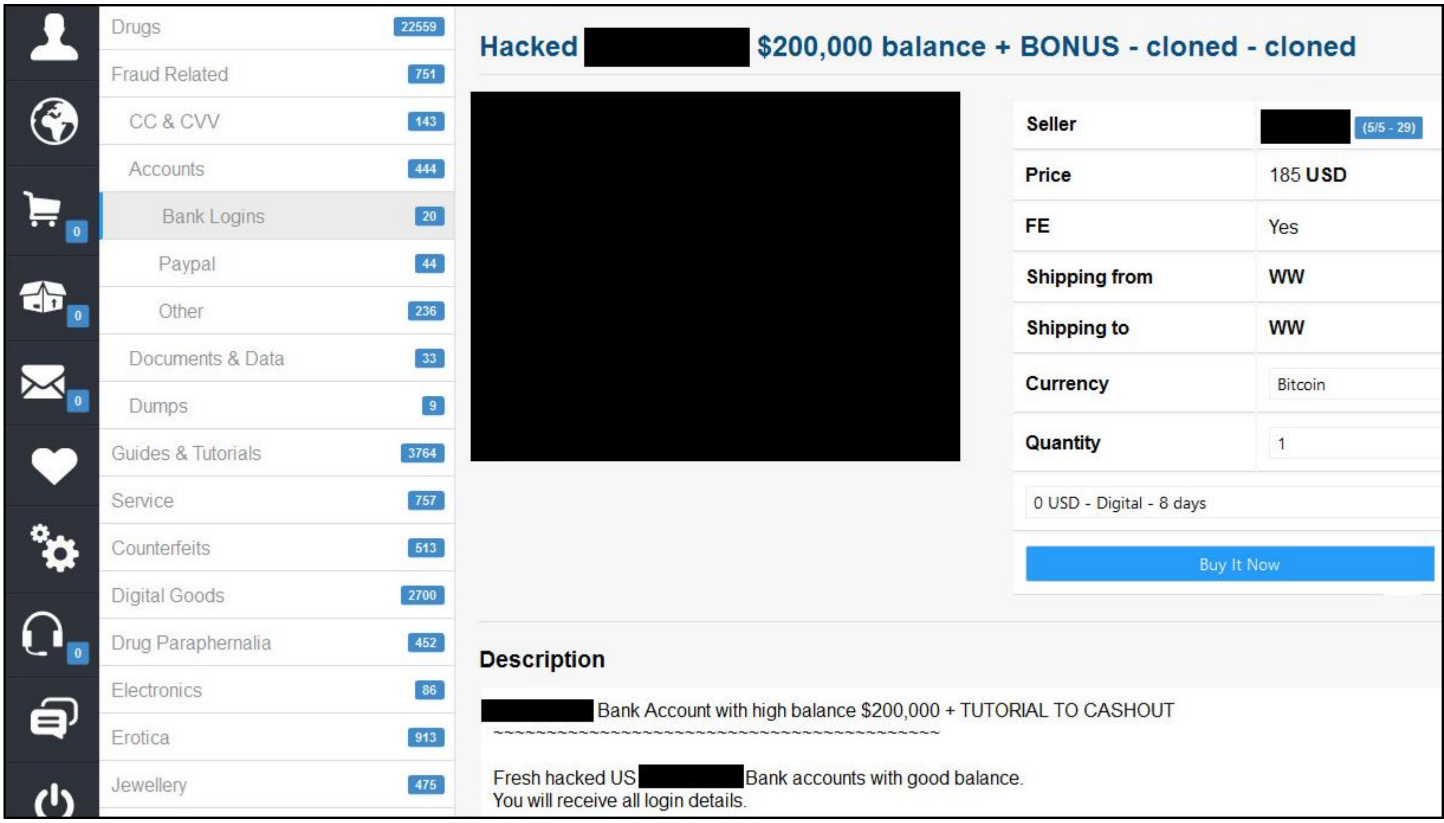
Top 5 Items for Sale on the Dark Web, and What Businesses Can Learn From Them

By Adam Meyer, chief security strategist, SurfWatch Labs

In April 2016, the dark web market Nucleus went offline. Before its disappearance, Nucleus had become the number two most popular market on the dark web, hosting tens of thousands of listings for a variety of illicit goods and services. The debate continues around why Nucleus vanished; however, it was just one of the many different markets where users could go to anonymously purchase credentials to customer accounts, stolen payment card data, pirated software, counterfeit currency and goods, malware, hacking services and more.

Knowing this can be quite useful to businesses and threat researchers. It can be leveraged for valuable cyber threat intelligence including the kind of data being bought and sold by cybercriminals, tools and services that are commonly used, and vulnerabilities that are being actively exploited. Most importantly, the dark web provides much needed context. But with the huge number of threats out there, some legitimate and some not, where should organizations focus their resources? Threat intelligence from the dark web can help provide businesses with that important insight. With that in mind, here are five of the most common items for sale on the dark web, and how that information can help organizations combat cybercrime, according to SurfWatch Labs.



Hacked [redacted] $200,000 balance + BONUS - cloned - cloned

[redacted]

Seller	[redacted] (5/5 - 29)
Price	185 USD
FE	Yes
Shipping from	WW
Shipping to	WW
Currency	Bitcoin
Quantity	1

0 USD - Digital - 8 days

Description

[redacted] Bank Account with high balance $200,000 + TUTORIAL TO CASHOUT
~~~~~~

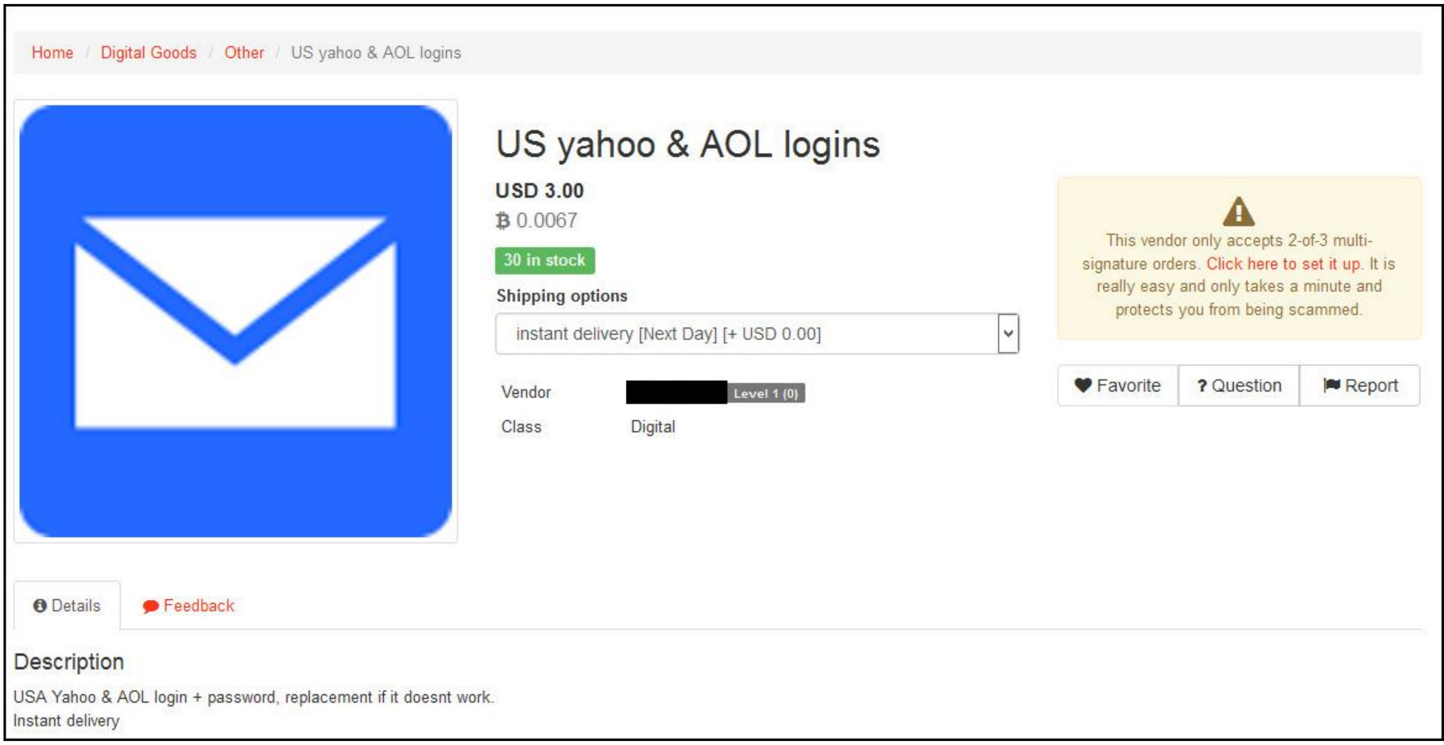
Fresh hacked US [redacted] Bank accounts with good balance.
You will receive all login details.

Screenshot of Nucleus Market before it went offline in May
~~~~~~

1.Stolen Credentials

Although a wide variety of cybercrime-related items are for sale on the dark web, stolen credentials are among the most prevalent. When looking at the most popular dark web market in 2016, credentials trade accounts for nearly a quarter of the data collected by SurfWatch Labs. Cybercriminals initially get this information by using phishing messages, malicious applications, and other methods to get malware such as keyloggers installed on victims' devices. These stolen usernames and passwords often end up for sale on the dark web where other malicious actors then use them for a variety of purposes. Although online banking accounts are a natural target, other types of credentials readily available for purchase include employee and personal email accounts, social media accounts, eBay and PayPal accounts, and other popular services such as Netflix, Uber, and more.

How this can help your organization: *With the huge number of data breaches and stolen credentials out there, it is likely that some employees have had their usernames and passwords compromised, and in many instances those include work-related email addresses. Monitoring the dark web for stolen credentials related to your brand and your employees can allow you to educate users, prevent fraudulent logins and stop a future attack from spreading.*



US yahoo & AOL logins

USD 3.00

฿ 0.0067

30 in stock

Shipping options

instant delivery [Next Day] [+ USD 0.00]

Vendor	[redacted] Level 1 (0)
Class	Digital

This vendor only accepts 2-of-3 multi-signature orders. Click here to set it up. It is really easy and only takes a minute and protects you from being scammed.

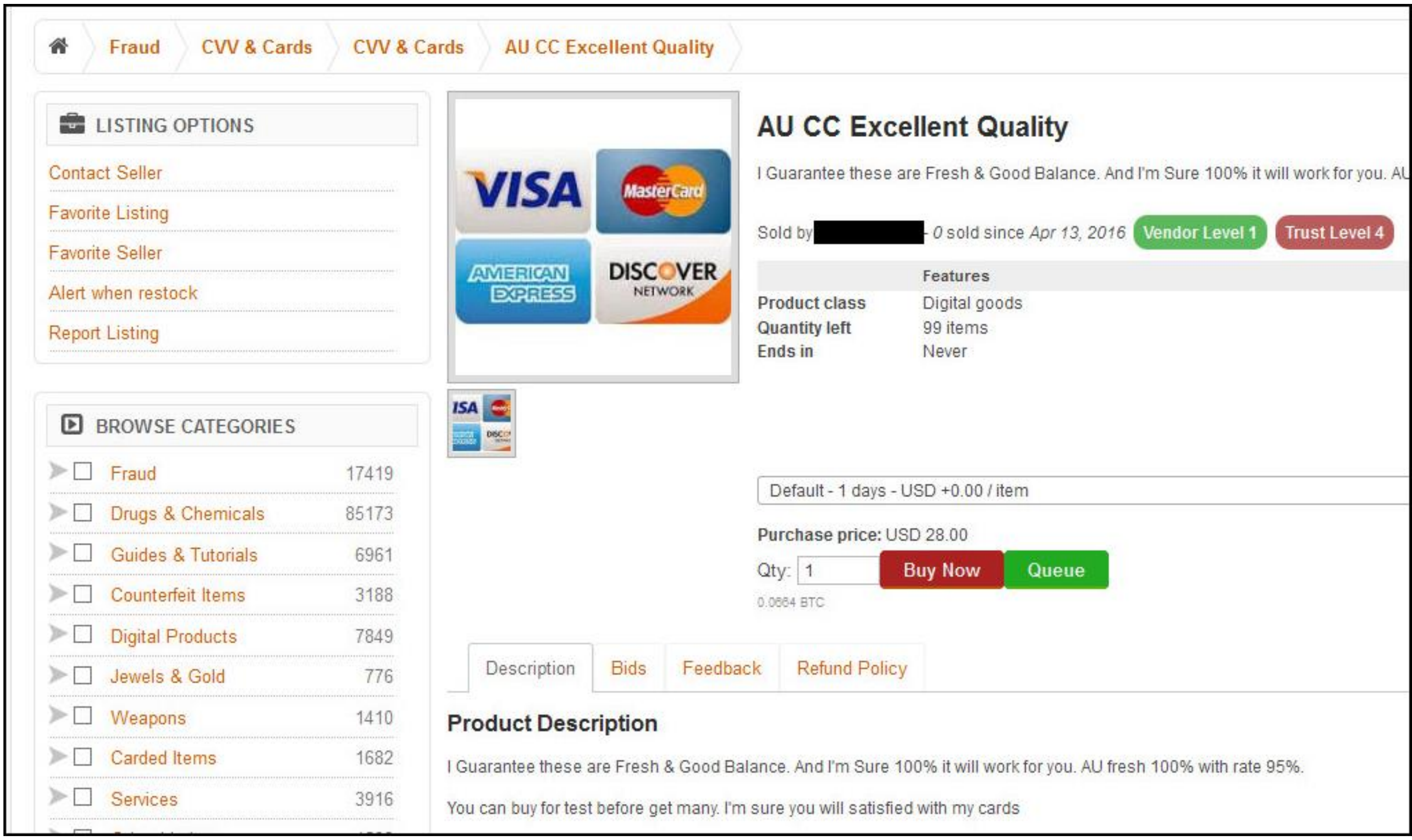
Description

USA Yahoo & AOL login + password, replacement if it doesnt work.
Instant delivery

2. Fraud and Stolen Identities

When a point-of-sale data breach occurs, that stolen payment card information often ends up for sale on various dark web markets. Cybercriminals act very quickly to monetize those accounts. The longer a stolen card is on the market, the less valuable it becomes due to the likelihood of it being tied to a data breach, theft, or other fraud -- and cancelled by the bank or cardholder. Other items for sale related to fraud include counterfeit documents such as passports and driver's licenses as well as personal information needed to open lines of credit such as Social Security numbers, dates of birth and other identifiers. Like traditional crime, cybercrime is largely driven by money, and fraud and stolen identities have traditionally been the go-to methods for turning a quick profit. However, it is not just the occasional thugs perpetrating these acts. It is often professional cybercrime rings run by gangs in other countries that have been perfecting their techniques for years.

How this can help your organization: *Many point-of-sale data breaches aren't discovered until the stolen payment card information shows up for sale or fraudulent charges begin occurring on enough cards to pinpoint a source of the compromise. By finding the stolen information sooner rather than later, retailers and financial institutions can shorten the shelf life of stolen cards and reduce potential losses.*



AU CC Excellent Quality

I Guarantee these are Fresh & Good Balance. And I'm Sure 100% it will work for you. AU

Sold by [redacted] - *0 sold since Apr 13, 2016* Vendor Level 1 Trust Level 4

	Features
Product class	Digital goods
Quantity left	99 items
Ends in	Never

Default - 1 days - USD +0.00 / item

Purchase price: USD 28.00

Qty: 1

0.0664 BTC

BROWSE CATEGORIES

□ Fraud	17419
□ Drugs & Chemicals	85173
□ Guides & Tutorials	6961
□ Counterfeit Items	3188
□ Digital Products	7849
□ Jewels & Gold	776
□ Weapons	1410
□ Carded Items	1682
□ Services	3916

Product Description

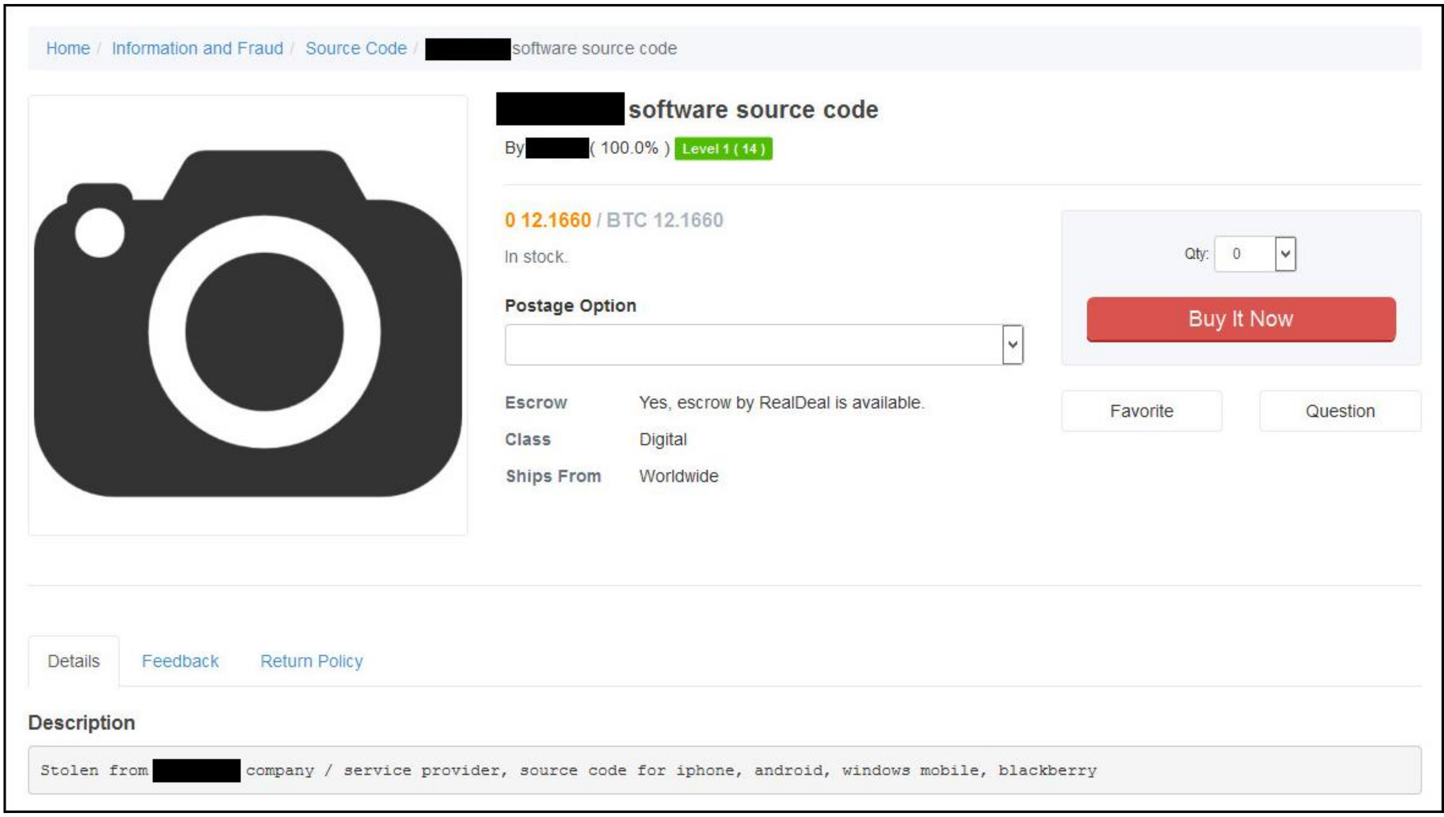
I Guarantee these are Fresh & Good Balance. And I'm Sure 100% it will work for you. AU fresh 100% with rate 95%.

You can buy for test before get many. I'm sure you will satisfied with my cards

3. Intellectual Property

Media piracy is a popular practice on the dark web. Stolen ebooks, music, movies and other forms of entertainment are sold at a fraction of the cost -- with none of the profits going to the creators. In addition to piracy, even more damaging forms of intellectual property are bought and sold on the dark web. This may include source code, stolen customer lists, trade secrets and other sensitive data stolen from organizations. A report by the Commission on the Theft of Intellectual Property stated that stolen intellectual property costs the United States as much as $300 billion each year, and the Center for Responsible Enterprise and Trade estimates trade secret theft costs between one and three percent of the GDP of advanced economies. Not all of that is sold on the dark web -- much of it is nation-state espionage -- however, of all the items for sale on the dark web, intellectual property tends to be the most impactful and have the most long-term consequences for organizations.

How this can help your organization: *Finding intellectual property such as source code for sale on the internet is a significant cause for concern. Unlike payment card information, which can be stolen from a variety of locations, intellectual property is a likely indicator of either an intruder gaining access or an insider selling valuable information. Media piracy, which is the most common form of intellectual property for sale, can lead to a significant loss of income, particularly if that item finds it's way onto popular torrent sites where users freely share stolen material.*



Home / Information and Fraud / Source Code / [redacted]software source code

[redacted] software source code

By [redacted](100.0%) Level 1 (14)

0 12.1660 / BTC 12.1660

In stock.

Postage Option

Qty: 0

Escrow Yes, escrow by RealDeal is available.

Class Digital

Ships From Worldwide

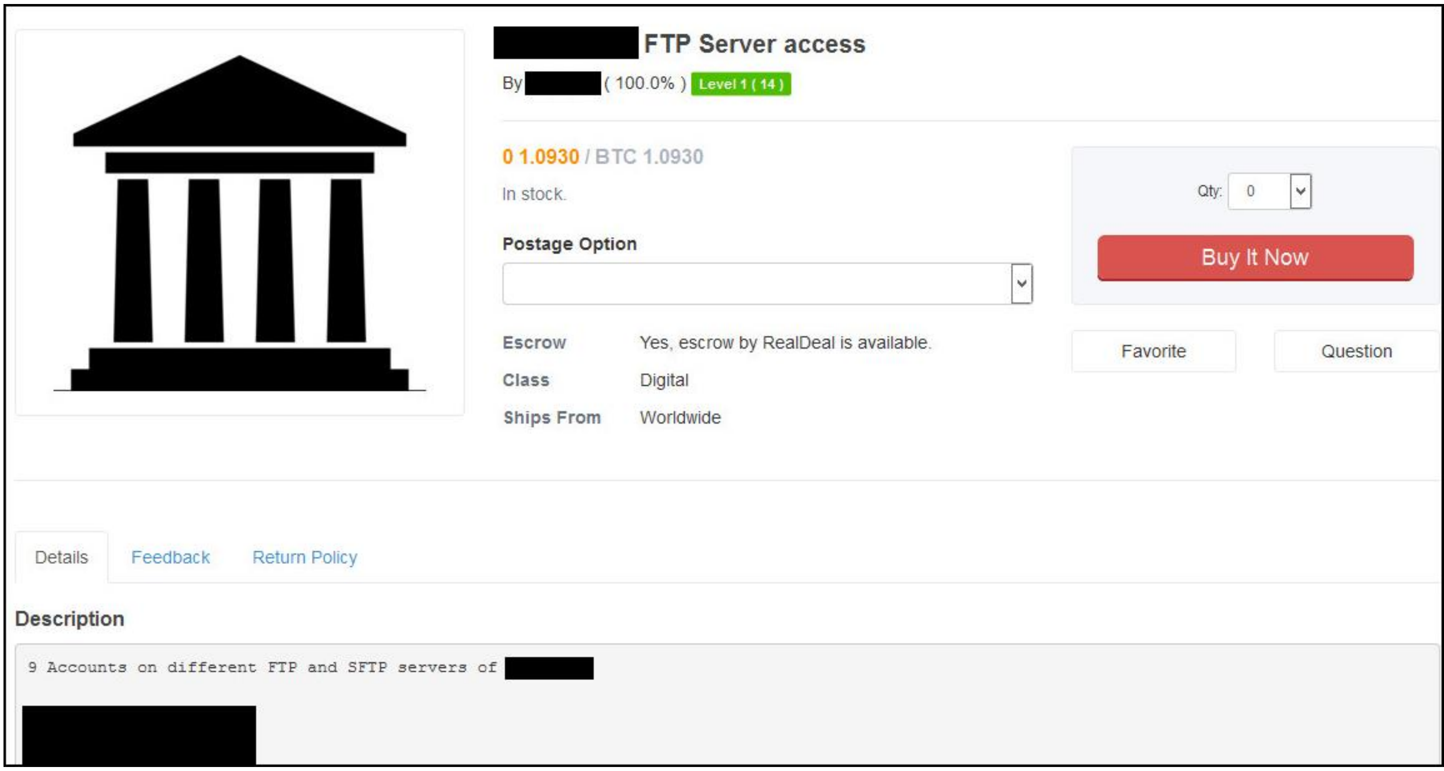
Description

Stolen from [redacted] company / service provider, source code for iphone, android, windows mobile, blackberry

4. Supply Chain Threats

Effective threat intelligence should include all the cyber risks facing an organization, including risk faced by third-party partners and vendors. Vendors may have their own credentials or intellectual property for sale on the dark web, or there may be relevant vulnerabilities that are being actively exploited by malicious actors. Those potential issues may move down the supply chain and impact other organizations along the way. For example, in April 2016 SurfWatch Labs threat intelligence analysts uncovered a breach into web hosting provider Invision Power Services, whose customers include professional sports leagues as well as major media and entertainment companies. A malicious actor indicated plans to infect those brands' users with malware. Although these incidents are often not the direct fault of those companies, the fallout from customers, investors and regulators does tend to fall directly at the feet of those organizations.

How this can help your organization: *Vendors and the supply chain are among the most common causes of data breaches, yet they're often a blind spot when it comes to an organization's cybersecurity practices. Having insight into potential issues not just within your organization, but with your partners can help to give a more complete picture of your organization's risk and help alert you to any potential issues before they make way down the supply chain and into your business.*



[redacted] FTP Server access

By [redacted] (100.0%) Level 1 (14)

0 1.0930 / BTC 1.0930

In stock.

Postage Option

Qty: 0

Escrow Yes, escrow by RealDeal is available.

Class Digital

Ships From Worldwide

Description

```
9 Accounts on different FTP and SFTP servers of [redacted]
```

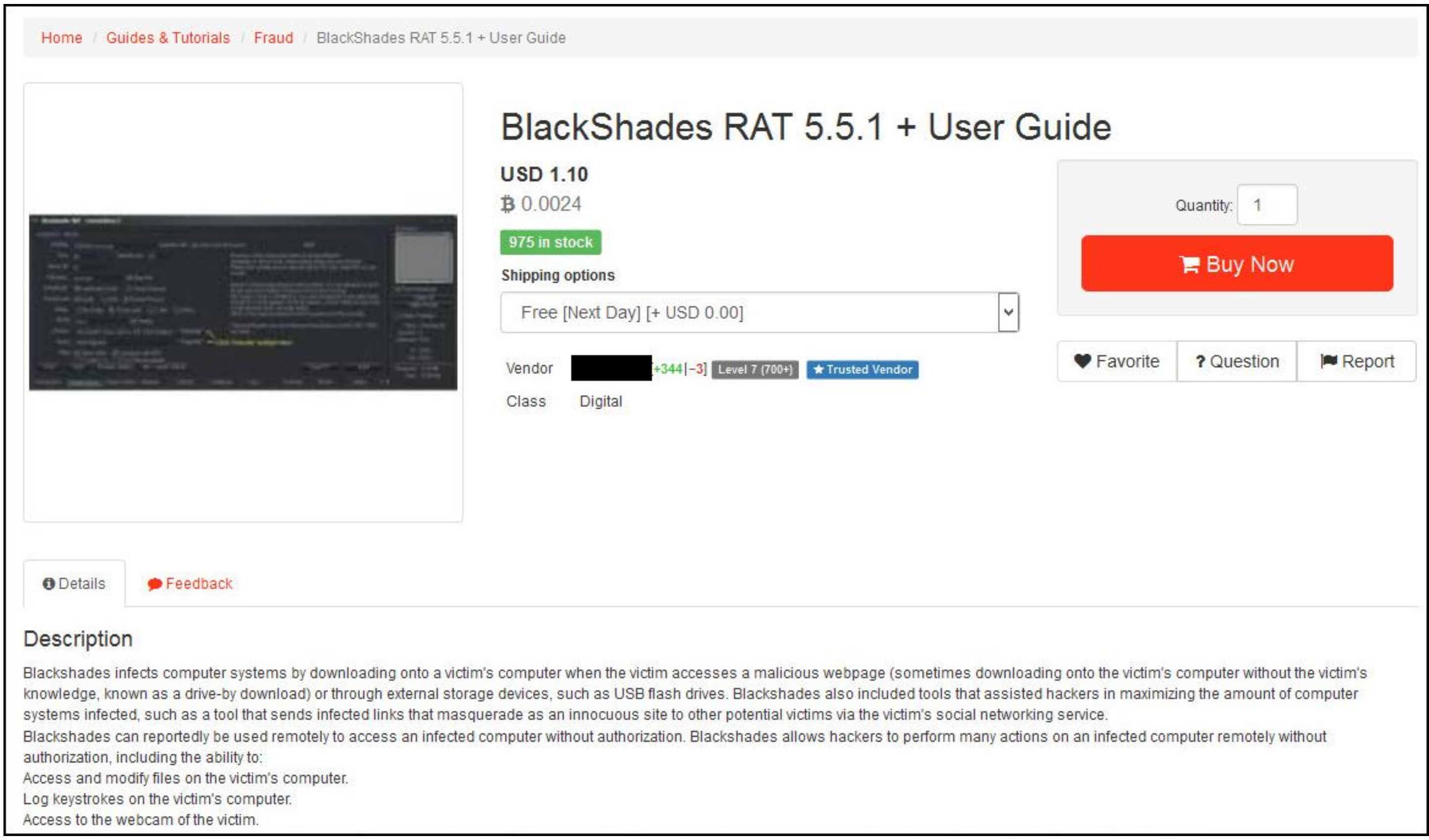
[redacted]

5. Hacking Tools and Services

In addition to stolen items, malicious actors can purchase many different types of hacking tools and services. One popular market actually began by specializing in selling zero-days and other rare exploits.

For example, one user was previously selling a new way to hack Apple iCloud accounts for $17,000. Other items for sale include exploit kits, keylogging malware, phishing pages, remote access Trojans, hacking guides and more. The cybercrime tools purchased may even come with subscription services, easy-to-use interfaces, technical support and other features often associated with legitimate software. In addition, cybercrime services are for sale including distributed denial-of-service attacks, doxing and help hacking accounts. The cybercrime-as-a-service model has segmented the market so that actors can specialize in their own field, whether that is running a botnet, creating exploit kits or stealing credentials. All types of cybercrime tools and services are available -- for a price.

***How this can help your organization:** Knowing what tools are readily available and popular can help organizations defend against common attack methods. In addition, new exploits that are put up for sale or modifications to existing tools can provide insight into how cybercriminals are evolving their attacks in order to evade detection. This context, combined with other dark web threats, can help provide the necessary threat intelligence to help effectively guide your organization's cyber risk management strategy.*



Home / Guides & Tutorials / Fraud / BlackShades RAT 5.5.1 + User Guide

BlackShades RAT 5.5.1 + User Guide

USD 1.10

฿ 0.0024

975 in stock

Shipping options

Free [Next Day] [+ USD 0.00]

Quantity: 1

Buy Now
Favorite
? Question
Report

Vendor [redacted] +344|−3] Level 7 (700+) ★ Trusted Vendor

Class Digital

Description

Blackshades infects computer systems by downloading onto a victim's computer when the victim accesses a malicious webpage (sometimes downloading onto the victim's computer without the victim's knowledge, known as a drive-by download) or through external storage devices, such as USB flash drives. Blackshades also included tools that assisted hackers in maximizing the amount of computer systems infected, such as a tool that sends infected links that masquerade as an innocuous site to other potential victims via the victim's social networking service.

Blackshades can reportedly be used remotely to access an infected computer without authorization. Blackshades allows hackers to perform many actions on an infected computer remotely without authorization, including the ability to:

Access and modify files on the victim's computer.

Log keystrokes on the victim's computer.

Access to the webcam of the victim.

Adam Meyer is chief security strategist at cyber threat intelligence firm, SurfWatch Labs. He may be reached at adam.meyer@surfwatchlabs.com