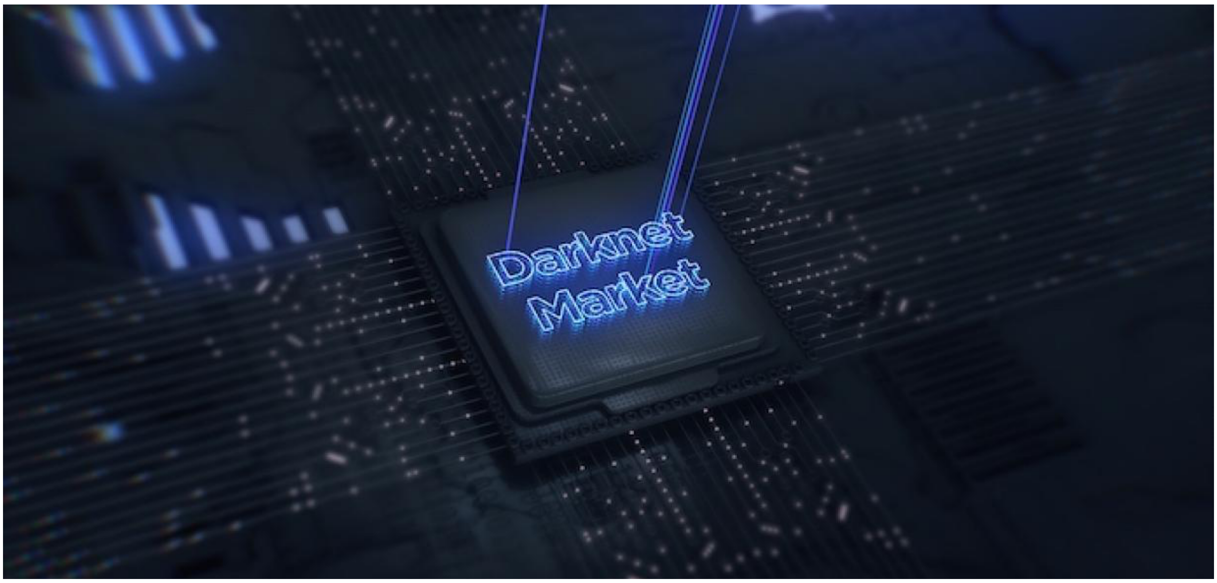
From Babuk Source Code to Darkside Custom Listings — Exposing a Thriving Ransomware Marketplace on the Dark Web

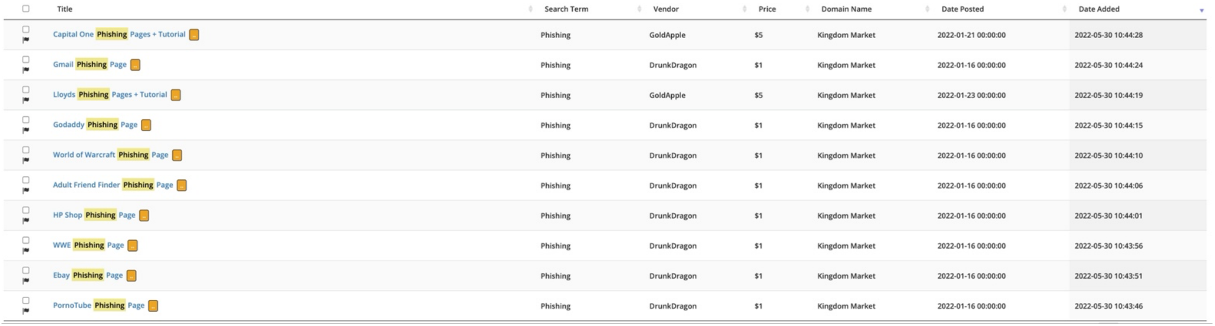


August 2, 2022 Shelley Boose

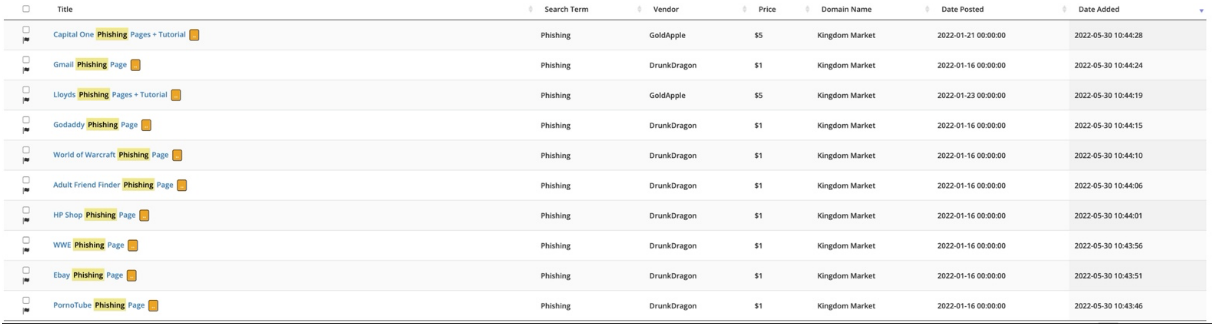
Venafi today announced the findings of a dark web investigation into ransomware spread via malicious macros. This comes in the wake of Microsoft's recent action on malicious macros spread via its Office applications.

Research: Venafi and Forensic Pathways

Conducted in partnership with criminal intelligence provider Forensic Pathways between November 2021 and March 2022, the research analyzed 35 million dark web URLs, including marketplaces and forums, using the Forensic Pathways Dark Search Engine. The findings uncovered 475 webpages of sophisticated ransomware products and services, with several high-profile groups aggressively marketing ransomware-as-a-service.



□	Title	Search Term	Vendor	Price	Domain Name	Date Posted	Date Added
□	Capital One Phishing Pages + Tutorial	Phishing	GoldApple	$5	Kingdom Market	2022-01-21 00:00:00	2022-05-30 10:44:28
□	Gmail Phishing Page	Phishing	DrunkDragon	$1	Kingdom Market	2022-01-16 00:00:00	2022-05-30 10:44:24
□	Lloyds Phishing Pages + Tutorial	Phishing	GoldApple	$5	Kingdom Market	2022-01-23 00:00:00	2022-05-30 10:44:19
□	Godaddy Phishing Page	Phishing	DrunkDragon	$1	Kingdom Market	2022-01-16 00:00:00	2022-05-30 10:44:15
□	World of Warcraft Phishing Page	Phishing	DrunkDragon	$1	Kingdom Market	2022-01-16 00:00:00	2022-05-30 10:44:10
□	Adult Friend Finder Phishing Page	Phishing	DrunkDragon	$1	Kingdom Market	2022-01-16 00:00:00	2022-05-30 10:44:06
□	HP Shop Phishing Page	Phishing	DrunkDragon	$1	Kingdom Market	2022-01-16 00:00:00	2022-05-30 10:44:01
□	WWE Phishing Page	Phishing	DrunkDragon	$1	Kingdom Market	2022-01-16 00:00:00	2022-05-30 10:43:56
□	Ebay Phishing Page	Phishing	DrunkDragon	$1	Kingdom Market	2022-01-16 00:00:00	2022-05-30 10:43:51
□	PornoTube Phishing Page	Phishing	DrunkDragon	$1	Kingdom Market	2022-01-16 00:00:00	2022-05-30 10:43:46



□	Title	Search Term	Vendor	Price	Domain Name	Date Posted	Date Added
□	Capital One Phishing Pages + Tutorial	Phishing	GoldApple	$5	Kingdom Market	2022-01-21 00:00:00	2022-05-30 10:44:28
□	Gmail Phishing Page	Phishing	DrunkDragon	$1	Kingdom Market	2022-01-16 00:00:00	2022-05-30 10:44:24
□	Lloyds Phishing Pages + Tutorial	Phishing	GoldApple	$5	Kingdom Market	2022-01-23 00:00:00	2022-05-30 10:44:19
□	Godaddy Phishing Page	Phishing	DrunkDragon	$1	Kingdom Market	2022-01-16 00:00:00	2022-05-30 10:44:15
□	World of Warcraft Phishing Page	Phishing	DrunkDragon	$1	Kingdom Market	2022-01-16 00:00:00	2022-05-30 10:44:10
□	Adult Friend Finder Phishing Page	Phishing	DrunkDragon	$1	Kingdom Market	2022-01-16 00:00:00	2022-05-30 10:44:06
□	HP Shop Phishing Page	Phishing	DrunkDragon	$1	Kingdom Market	2022-01-16 00:00:00	2022-05-30 10:44:01
□	WWE Phishing Page	Phishing	DrunkDragon	$1	Kingdom Market	2022-01-16 00:00:00	2022-05-30 10:43:56
□	Ebay Phishing Page	Phishing	DrunkDragon	$1	Kingdom Market	2022-01-16 00:00:00	2022-05-30 10:43:51
□	PornoTube Phishing Page	Phishing	DrunkDragon	$1	Kingdom Market	2022-01-16 00:00:00	2022-05-30 10:43:46

Darkside Ransomware Marketplace / Credit: Forensic Pathway, Venafi

Results:

- **87% of the ransomware found on the dark web has been delivered via malicious macros to infect targeted systems.**
- **30 different "brands" of ransomware were identified within marketplace listings and forum discussions.**
- **Many strains of ransomware being sold — such as Babuk, GoldenEye, Darkside/BlackCat, Egregor, HiddenTear and WannaCry — have been successfully used in high-profile attacks.**
- **Ransomware strains used in high-profile attacks command a higher price for associated services. For example, the most expensive listing was $1,262 for a customized version of Darkside ransomware, which was used in the infamous Colonial Pipeline ransomware attack of 2021.**
- **Source code listings for well-known ransomware generally command higher price points, Babuk source code is listed for $950 and Paradise source code is selling for $593.**

"Ransomware continues to be one of biggest cybersecurity risks in every organization," said Kevin Bocek, vice president of security strategy and threat intelligence for Venafi. "The ransomware attack on Colonial Pipeline was so severe that it was deemed a national security threat, forcing President Biden to declare a national state of emergency."

Microsoft action

Macros are used to automate common tasks in Microsoft Office, helping people to be more productive. However, attackers can use this same functionality to deliver many kinds of malware, including ransomware. In February, Microsoft announced it would disable VBA macros obtained from the Internet. But they temporarily reversed that decision in response to community feedback. (In July, Microsoft reinstated its policy of disabling VBA macros.)

“Given that almost anyone can launch a ransomware attack using a malicious macro, Microsoft's decision to roll back the disabling of macros should scare the pants off everyone,” said Bocek.

Tools allow attacks with minimal technical skills

In addition to a variety of ransomware at various price points, the research also uncovered a wide range of services and tools that help make it easier for attackers with minimal technical skills to launch ransomware attacks. Services with the greatest number of listings include those offering source code, build services, custom development services, and ransomware packages that include step-by-step tutorials.

Generic ransomware build services also command high prices, with some listings costing more than $900. At the other end of the price spectrum, many low-cost ransomware options are available across multiple listings — with prices starting at just $0.99 for Lockscreen ransomware.

Venafi can help

These findings are another example of the need for a machine identity management control plane to drive specific business outcomes including observability, consistency, and reliability. In particular, code signing is a key machine identity management security control that eliminates the threat of macro-enabled ransomware.

“Using code signing certificates to authenticate macros means that any unsigned macros cannot execute, stopping ransomware attacks in its tracks,” Bocek concludes. “This is an opportunity for security teams to step up and protect their businesses, especially in banking, insurance, healthcare and energy where macros and Office documents are used every day to power decision making.”

About the research:

This research was carried out between November 2021-March 2022 by Venafi in partnership with Forensic Pathways, which has developed Dark Search Engine (DSE), an automated crawler/scraper of the Tor. Onion Dark Web. The intelligence tool contains >35 million URLs in the index.

Publicly available information, such as PC Risk, was used to determine if malicious macros were used in the initial attack vector.

About Forensic Pathways:

Incorporated in 2001 Forensic Pathways provides innovative technologies within the criminal intelligence arena. Focused primarily on the provision of digital forensic technologies, Forensic Pathways offers its international clients unique technologies in the management of mobile phone data, image analysis and ballistics analysis.