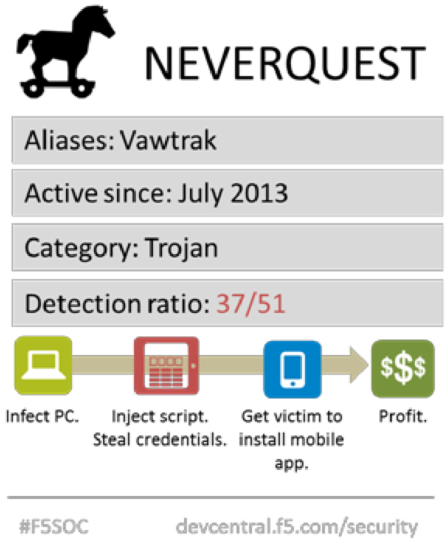
F5 SOC Malware Summary Report: Neverquest

Lori MacVittie, 2014-02-09

#F5SOC #malware #2FA #infosec The good news is that compromising #2FA requires twice the work. The bad news? Malware can do it.



That malware is a serious problem, particularly for organizations that deal with money, is no surprise. Malware is one of the primary tools used by fraudsters to commit, well, fraud.

In 2013, the number of cyberattacks involving malware designed to steal financial data rose by 27.6% to reach 28.4 million according to noted security experts at Kaspersky. Organizations felt the result; 36% of financial institutions admit to experiencing ACH/wire fraud (2013 Faces of Fraud Survey).

To protect against **automated** transactions originating from infected devices, organizations often employ two-factor authentication (2FA) that leverages OTP (one time passwords) or TAN (transaction authorization numbers) via a secondary channel such as SMS to (more) confidently verify identity. 2FA systems that use a secondary channel (a device separate from the system on which the transaction is initiated) are more secure, naturally, than those that transmit the second factor over a channel that can be used from the initiating system, a la an e-mail.

While 2FA that use two disparate systems are, in fact, more secure, they are not foolproof, as malware like Neverquest has shown.

Neverquest activity has been seen actively in the wild, meaning despite the need to compromise two client devices - usually a PC/laptop and a smartphone - it has been successful at manipulating victims into doing so. The primary infection occurs via the PC, which is a lot less difficult these days thanks to the prevalence of infected sites. But the secondary infection requires the victim to knowingly install an app on their phone, which means convincing them they should do so.

This is where script injection comes in handy.

Malware of this ilk modify the web app by injecting a script that changes the behavior and/or look of the page. Even the most savvy browsers are unlikely to be aware of such changes as they occur "under the hood" at the real, official site. Nothing about the URI or host changes, which means all appears as normal. The only way to detect such injections is to have prior knowledge of what the page *should* look like - down to the code level.

The trust a victim has for the banking site is later exploited with a popup indicating they should provide their phone number and download an app. As it appears to be a valid request coming from their financial institution, victims may very well be tricked into doing so.

And then Neverquest has what it needs - access to SMS messages over which OTP and/or TAN are transmitted. The attacker can then initiate **automated** transactions and confirm them by intercepting the SMS messages. Voila. Fraud complete.

We (as in the corporate We) rely on our F5 SOC (Security Operations Center) team to analyze malware to understand how they compromise systems and enable miscreants to carry out their fraudulent goals. In July, the F5 SOC completed its analysis of Neverquest and has made its detailed results available. You can download the full technical analysis here on DevCentral.

We've also made available a summary analysis that provides an overview of the malware, how it works, and how its risk can be mitigated. You can get that summary here on DevCentral as well.

The F5 SOC will continue to diligently research, analyze and document malware in support of our security efforts and as a service to the broader community. We hope you find it useful and informative, and look forward to sharing more analysis in the future.

You can get the summary analysis here, and the full technical analysis here.

Additional Resources:

- F5 SOC on DevCentral
- F5 WebSafe Service
- F5 Web Fraud Protection Reference Architecture