Shylock's New Trick: Evading Malware Researchers

securityintelligence.com/shylocks-new-trick-evading-malware-researchers/

November 28, 2012

Home / Banking & Finance

Shylock’s New Trick: Evading Malware Researchers

Banking & Finance November 28, 2012
By Dana Tamir 2 min read

Shylock is a financial malware platform discovered by IBM Security in 2011. Like most malware strains, it continues to evolve in order to bypass new defensive technologies put in place by financial institutions and enterprises. While analyzing a recent Shylock dropper, we noticed a new trick it uses to evade detection. Namely, it can identify and avoid remote desktop environments, a setup commonly used by researchers when analyzing malware.

Exploiting the Lab

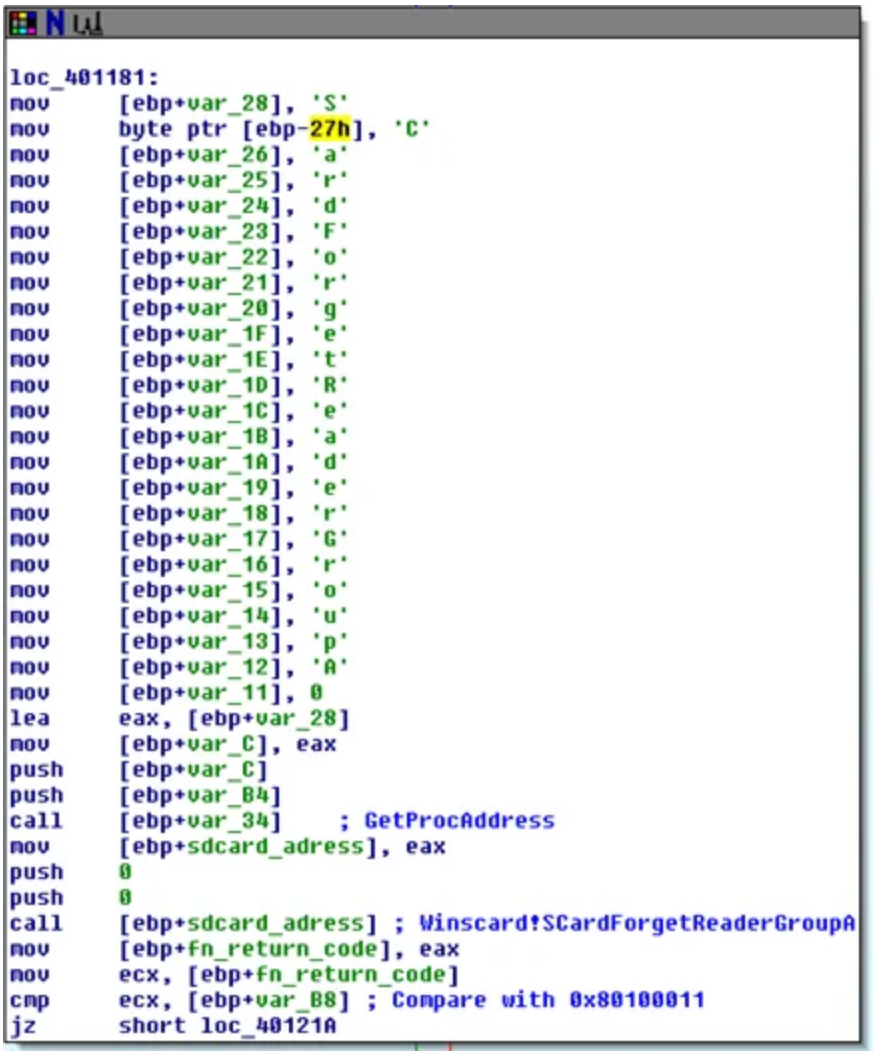
Researchers collect suspected malware samples for analysis and often place them onto machines that are isolated in an operations center, also known as a lab. Rather than sit in front of a rack of physical machines in a cold basement lab, researchers use remote desktop connections to study malware from the convenience and coziness of their offices. It is this human weakness that Shylock exploits. We have discovered advanced malware that is now capable of detecting remote desktop environments to evade researchers.

The Shylock dropper we discovered detects a remote desktop environment by feeding invalid data into a certain routine and then observing the error code returned. It uses this return code to differentiate between normal desktops and other lab environments. In particular, when executed from a remote desktop session, the return code will be different and Shylock won't install. It is possible to use this method to identify other known or proprietary virtual/sandbox environments, as well.

For those more technically oriented, here is a bit more detail. The dropper dynamically loads Winscard.dll and calls the function SCardForgetReaderGroupA(0, 0). The malware proceeds as expected only if the return value is either 0x80100011 (SCARD_E_INVALID_VALUE) or

0x2 (ERROR_FILE_NOT_FOUND).

We noticed that when the dropper is executed locally, the return value is 0x80100011, but when it is executed from a remote desktop session the return value is 0x80100004 (SCARD_E_INVALID_PARAMETER). The assembly language source code is shown below. We have found a number of malware strains that utilize different approaches to identify specific execution environments in order to take appropriate evasive actions. The assembly language source code is shown below.



```
loc_401181:
mov     [ebp+var_28], 'S'
mov     byte ptr [ebp-27h], 'C'
mov     [ebp+var_26], 'a'
mov     [ebp+var_25], 'r'
mov     [ebp+var_24], 'd'
mov     [ebp+var_23], 'F'
mov     [ebp+var_22], 'o'
mov     [ebp+var_21], 'r'
mov     [ebp+var_20], 'g'
mov     [ebp+var_1F], 'e'
mov     [ebp+var_1E], 't'
mov     [ebp+var_1D], 'R'
mov     [ebp+var_1C], 'e'
mov     [ebp+var_1B], 'a'
mov     [ebp+var_1A], 'd'
mov     [ebp+var_19], 'e'
mov     [ebp+var_18], 'r'
mov     [ebp+var_17], 'G'
mov     [ebp+var_16], 'r'
mov     [ebp+var_15], 'o'
mov     [ebp+var_14], 'u'
mov     [ebp+var_13], 'p'
mov     [ebp+var_12], 'A'
mov     [ebp+var_11], 0
lea     eax, [ebp+var_28]
mov     [ebp+var_C], eax
push    [ebp+var_C]
push    [ebp+var_B4]
call    [ebp+var_34]    ; GetProcAddress
mov     [ebp+sdcard_adress], eax
push    0
push    0
call    [ebp+sdcard_adress] ; Winscard!SCardForgetReaderGroupA
mov     [ebp+fn_return_code], eax
mov     ecx, [ebp+fn_return_code]
cmp     ecx, [ebp+var_B8] ; Compare with 0x80100011
jz      short loc_40121A
```

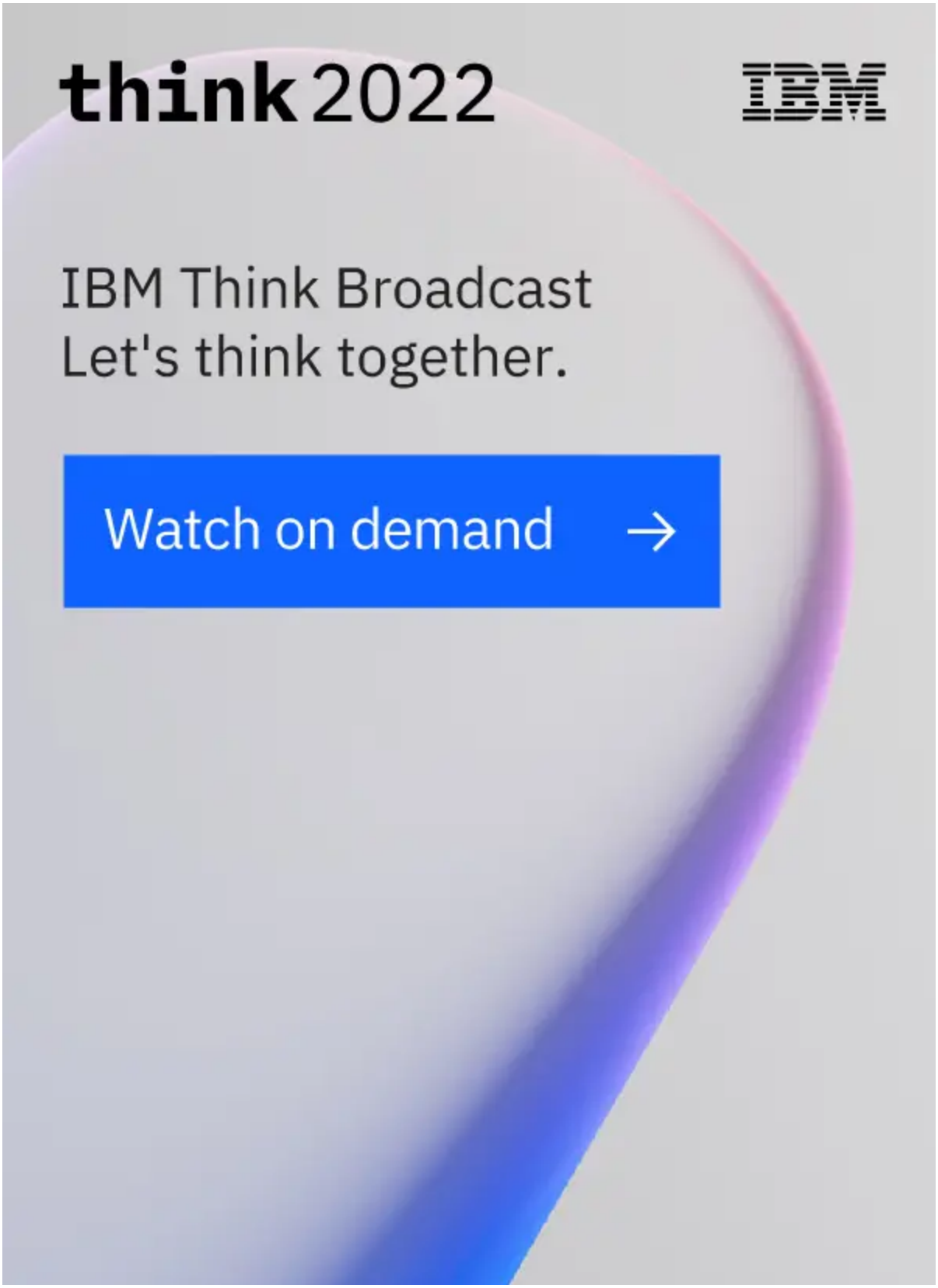
IBM vs. Shylock

IBM Security solutions are not affected by anti-VM/anti-research techniques employed by malware. This is because we use real-time application protection to monitor for suspected malware behavior in the endpoint device's memory. This approach prevents malware from compromising applications, including the browser, and stealing data like user credentials. It is also immune to malware evasion techniques designed to identify remote desktop and virtual machine environments.

Financial Malware | Malware | Sandbox | Shylock

Dana Tamir
Director of Enterprise Security at Trusteer, an IBM Company

Dana Tamir is Director of Enterprise Security at Trusteer, an IBM Company. In her role she leads activities related to enterprise advanced threat protection ...



more from Banking & Finance

Banking & Finance May 10, 2022

What Do Financial Institutions Need to Know About the SEC's Proposed Cybersecurity Rules?

On March 9, the U.S. Securities and Exchange Commission (SEC) announced a new set of proposed rules for cybersecurity risk management, strategy and incident disclosure for public companies. One intent of the rule changes is to provide “consistent, comparable and decision-useful” information to investors. Not yet adopted, these new rules – published in the Federal […]

Advanced Threats May 9, 2022

New DOJ Team Focuses on Ransomware and Cryptocurrency Crime

While no security officer would rely on this alone, it’s good to know the U.S. Department of Justice is increasing efforts to fight cyber crime. According to a recent address in Munich by Deputy Attorney General Lisa Monaco, new efforts will focus on ransomware and cryptocurrency incidents. This makes sense since the X-Force Threat Intelligence […]

Banking & Finance May 3, 2022

SEC Proposes New Cybersecurity Rules for Financial Services

Proposed new policies from the Securities and Exchange Commission (SEC) could spell changes for how financial services firms handle cybersecurity. On Feb. 9, the SEC voted to propose cybersecurity risk management policies for registered investment advisers, registered investment companies and business development companies (funds). Next, the proposal will go through a public comment period until […]

Banking & Finance April 19, 2022

Top Security Concerns When Accepting Crypto Payment

From Microsoft to AT&T to Home Depot, more companies are accepting cryptocurrency as a way to pay for products and services. This makes perfect sense as crypto coins are a viable revenue source. Perhaps the time is ripe for businesses to learn how to receive, process and convert crypto payments into fiat currency. Still, many [...]

Analysis and insights from hundreds of the brightest minds in the cybersecurity industry to help you prove compliance, grow business and stop threats.