TrickBot

1. **What is it?**

TrickBot specializes in stealing banking credentials. It is an enhanced trojan malware evolved from Emotet Malware that became the top threat attackers employed to penetrate organizational business.

1. **When was it first detected?**

2016

1. **What does it do?**

A spear-phishing email disguised as unpaid invoices, requests to update an account, contains a malicious download link or an attached, macro-enabled, Word or Excel document. Once the link or attachment is opened it will prompt the end-user to enable the doc, which executes a VBScript to run a PowerShell script to download the malware. TrickBot runs checks to ensure it is not in a sandbox environment and then attempts to disable antivirus programs such as Microsoft Windows Defender. Once executed, TrickBot redeploys itself in the "%AppData%" folder and creates a scheduled task that provides persistence.

1. **How is it detected?**

Network Admins may notice changes in traffic or attempts to reach out to blacklisted IPs and domains, as the malware will communicate with TrickBot’s command and control infrastructure to exfiltrate data and receive tasks.

1. **How is it removed?**

The IT team can isolate, patch, and remediate each infected system.

1. **How can you defend against it?**

Security awareness training program: detection and reporting.

Periodical drills with follow up findings and education.

Software updates and operating system patching.

Updated antivirus software.

Isolate the infected machine and reset passwords.

1. **Facts found along the way:**

2018 study by Osterman Research 76% of organizations have experienced a phishing attack or witnessed spear-phishing.

"Based on our research not only is TrickBot one of the most prominent organized crime gangs in the bank fraud arena, we also expect to see it maintain its position on the global malware chart, unless it is interrupted by law enforcement in 2019." Limor Kessem Global Executive Security Advisor, IBM

Sources:

[CyberSecurity Alert: TrickBot Malware](https://www.youtube.com/watch?v=bXRAY945MyE)

[How Trickbot Works](https://www.youtube.com/watch?v=2MUKoNcGo-8)

[TrickBot Takes Over as Top Organizational Threat](https://www.youtube.com/watch?v=wIyYsTJliMA)

<https://security.radware.com/ddos-knowledge-center/ddospedia/trickbot/>

<https://blog.malwarebytes.com/detections/trojan-trickbot/>