Microsoft
THREAT INTELLIGENCE

NOTE: The data in this document is provided to you subject to the following conditions: Your organization may use the data solely for informational, remediation, and defensive purposes. The data may be inaccurate and/or may refer to legitimate but compromised properties. THIS DOCUMENT IS PROVIDED "AS-IS" AND FOR INFORMATIONAL PURPOSES ONLY. MICROSOFT DISCLAIMS ALL EXPRESS, IMPLIED, OR STATUTORY WARRANTIES. THIS INCLUDES THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT.

MSTI Activity Alert – Human-Operated Ransomware Threat to Healthcare

NOTE: Microsoft notifies any customers that are targeted or compromised by the activity described in this report. This update is for advisory purposes only.

Trickbot was first spotted in 2016 as a banking trojan and designed to steal credentials from online banks and financial services. Over the years, Trickbot's operators were able to build a sophisticated attack infrastructure which evolved into a modular payload available for malware-as-a-service. Microsoft tracks a cluster of threat actor activity related to the Trickbot ecosystem that has been responsible for a significant amount of human-operated campaigns[1] including attacks that steal credentials, exfiltrate data, and deploy additional payloads, most notably Cobalt Strike beacon and Ryuk[2] ransomware, in target networks.

In recent attacks involving Trickbot, the time from initial compromise to enterprise-wide ransomware deployment has dropped significantly and is often 24-48 hours or less in some cases. These threat actors have used the malware families publicly referred to as "BazaLoader/KEGTAP" to initially compromise victims.

This summary is part of a deeper analysis of Trickbot, published in the following recent blog posting: https://www.microsoft.com/security/blog/2020/10/12/trickbot-disrupted/

Microsoft also recently took action against this activity and published the following blog posting: https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/

Microsoft is distributing this Activity Alert to customers within the healthcare industries to share important information toward assisting in the identification or defense of customer assets.

Activity description

Microsoft is aware of Trickbot infrastructure actively targeting customers in the healthcare sector. Trickbot commonly targets customers with sophisticated malware and human-operated ransomware attacks.

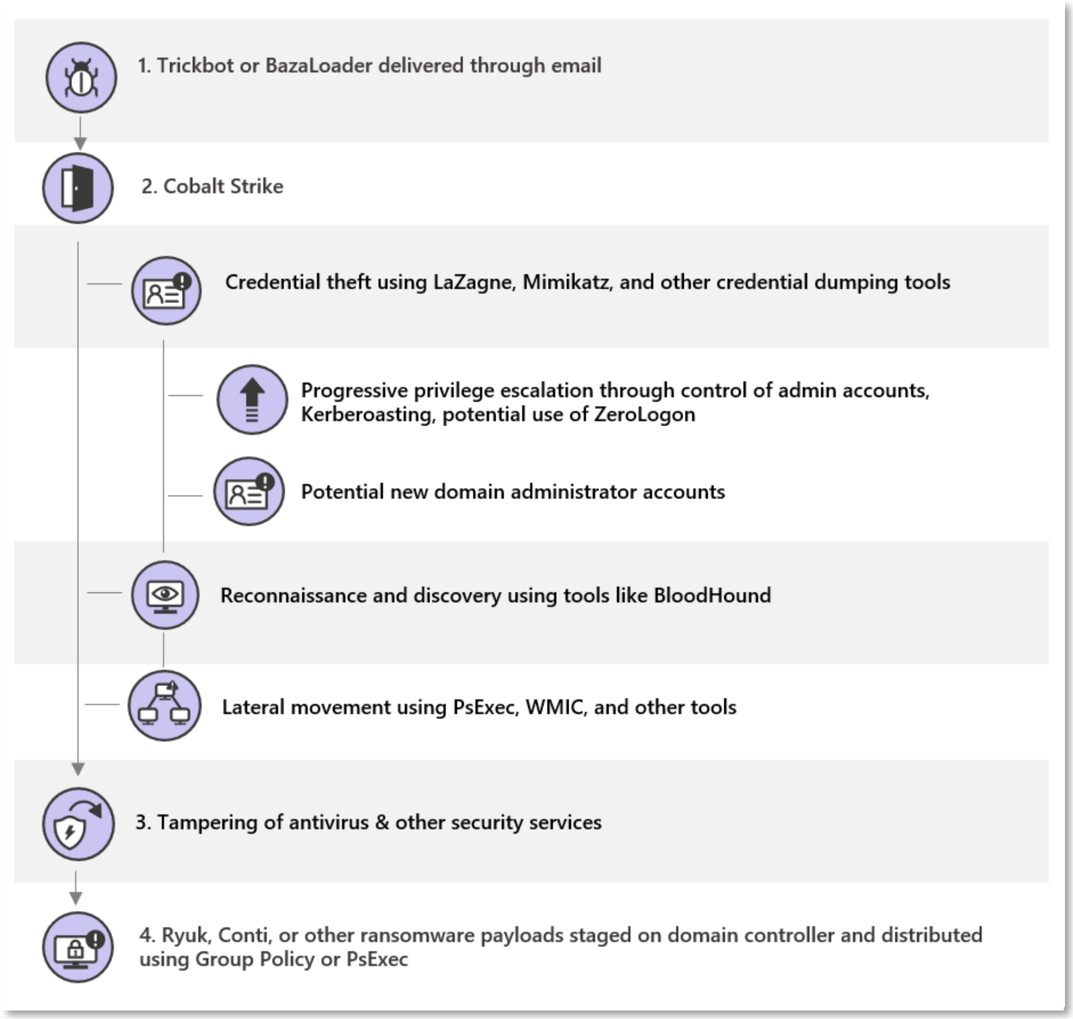
- The actors gain initial access through Trickbot or BazaLoader/KEGTAP.
- The actors will then move to human-operated phases involving credential theft and lateral movement.
- Finally, the actors will use stolen domain admin or other privileged credentials to deploy a ransomware payload through PsExec or Group Policy.

It is critical that customers implement protections using the IOCs accompanying this document and hardening guidance as quickly as possible to minimize potential impact to their business operations.

[1] https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

[2] https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/

Figure 1: Example of attack chain involving Trickbot to deliver ransomware


1. Trickbot or BazaLoader delivered through email
2. Cobalt Strike
Credential theft using LaZagne, Mimikatz, and other credential dumping tools
Progressive privilege escalation through control of admin accounts, Kerberoasting, potential use of ZeroLogon
Potential new domain administrator accounts
Reconnaissance and discovery using tools like BloodHound
Lateral movement using PsExec, WMIC, and other tools
3. Tampering of antivirus & other security services
4. Ryuk, Conti, or other ransomware payloads staged on domain controller and distributed using Group Policy or PsExec

Indicators of compromise (IOCs)

NOTE: The associated IOCs observed during this activity are included in an appended CSV file.

Microsoft encourages customers to implement detections and protections that will assist in identifying possible prior campaigns or prevent future campaigns against their systems.

Analyst's comment: These indicators should not be considered exhaustive for this observed activity.

Recommended defenses

These actors often rely on RDP brute-force, systems with known security vulnerabilities, and weak application settings to gain initial access into a target network. The actors then move laterally to deploy payloads, turning off security solutions along the way. Hardening your network in these focus areas can significantly reduce the chance of attacker success and ability to distribute ransomware.

- ***Block out-bound traffic to the IP addresses noted in the attached CSV***
- ***Sinkhole/blocklist the domains noted in the attached CSV***
- ***Randomize local administrator passwords***

  Use of the Local Administrator Password Solution (LAPS) provides management of local account passwords of domain joined computers. Passwords are stored in Active Directory (AD) and protected by ACL, so only eligible users can read it or request its reset.
- ***Avoid using privileged accounts like Domain Administrator to run services or scheduled tasks.***

  The actors frequently rely on cached credentials from the LSA Secrets to elevate privileges. If you are unsure if you have this configuration in your environment, you can utilize Windows Logon Events to determine your exposure—look for 4624 events of the highly privileged accounts where the logon type is 4 or 5
- ***Patch for recent vulnerabilities especially CVE-2020-1472 also known as ZeroLogon.***

  The adversaries associated with this activity have used unpatched systems to elevate privileges. If you have not yet implemented CVE-2020-1472 patch and experienced a Trickbot or BazaLoader infection, investigate for evidence of use of tools such as Mimikatz to exploit the vulnerability and treat the domain as compromised if discovered.
- ***Block lateral movement between workstations with a host firewall.***

  The adversary relies on tools like Cobalt Strike, PsExec, and WMI lateral movement to move between systems. Blocking RPC and SMB communications between workstations and servers can slow their ability to spread. Enterprise customers can use attack surface reduction rule "Block process creations originating from PsExec and WMI commands," if the host firewall is not possible.
- ***Prioritize specific Detections***

  Treat any detections associate of Cobalt Strike, Suspicious Decoded Content, and Atosev as high severity and address immediately.
- ***Enable multi-factor authentication.***

  Enable multi-factor authentication (MFA) across both business and personal email accounts to thwart most credential harvesting attacks. Blog: Your password doesn't matter--but MFA does!
- ***Support for Microsoft Threat Experts customers***

  Microsoft Threat Experts customers can work with their designated contacts to track this or other new and emerging threats. Microsoft Threat Experts will regularly review event logs and other signals using their dynamic collection of threat intelligence and provide additional expert insights.