Financial Trojan GozNym

This is a security alert for all TruShield clients, the financial services industry, and the community at large. We have learned of a new Trojan called GozNym. GozNym is targeting banks and financial institutions.

Introduction

As anticipated, financial institutions remain a popular target of opportunity for cybercriminals. GozNym is one of the latest in a steady stream of threats leveled at business banks, credit unions, ecommerce, and more. One unique quality about GozNym, as indicated by the name of the Trojan, is that it incorporates elements of two other Trojans targeting the same industry. Additionally, the geographical scope of targets currently is largely within the U.S., with a few outliers in Canada. To date there have been a total of at least 24 entities targeted in the financial services industry and an estimated $4 million in losses in early April.

Mixing Old Tricks

The two malware strains combined to produce GozNym are known as Gozi ISFB and Nymaim. Researchers at IBM X-Force observed that the first stage employs the tactics of Nymaim, by focusing on a stealthy and persistent approach with less emphasis on the previously used ransomware lock screen method. These tactics were quite successful in the past, and in late 2013 it was reported that over 2.5 million infections by this Trojan were seen. In the second stage of execution, GozNym uses Gozi ISFB functionality against online banking, as seen near the close of 2015. Determination that these two were hybridized into GozNym is not only possible by noting similar tactics, but also examination of the source code. One specific example for comparative analysis is the old Gozi ISFB web injection DLL vs GozNym's new buffer. The newer buffer is definitely altered in terms of size, but performs essentially the same function with relation to web sessions.

State of Industry Security

GozNym represents just one small example of the increasing complexity of many threats poised to strike at the financial services industry. It's important to note that even transitions to newer operating systems like Windows 10 did not impede the older families from altering to match. Financial institutions need to take immediate action to address any security gaps that would allow GozNym to wreak havoc, since this is a

preventable threat employing only slightly altered methods. Even organizations prepared for GozNym should consider additional options and redundancies. As 2016 continues it would not be surprising to see a wave of more complex malware build on these tactics against the financial services industry.

Indicators of Compromise

MD5 Hash
2A9093307E667CDB71884ECC1B480245
F652FF6F745AC302E7067E5A347BB644
B954391BC225C662D4720BC8AE5F95CC
0058B5A2CBF64B536EA15C390E60DE20
58D893C9074233D83AE694A180A28D01
C5AB408B9F710EBD63A515217A975274
47BD2478FEB9CB0C08F7E716C94CC8C8
F1A12884B999B9E572F91A94043D6E01
F232CFFA7802E54141F6F46691039E4B
44d09EAC8CF488000FB8AB3585789B5B
2CD713AD63B5D9FE53000F2362D85FC9
57944BA9A7EBDD2CED0F53779582EA73
9C17BD1DAC02FF0FB5608D388A4F0797
C41FFC1FD6E3F5157181B6E45F45F4FE
1BA77419AACBD0360EBC24E06CF2BB1C
C2s
194.149.138.49
54.186.122.88
82.13.46.90
168.235.72.204
59.116.23.197
165.203.213.15
21.221.249.200
33.38.160.238
165.203.213.15
21.26.242.199
33.38.160.238
21.45.165.216
208.104.191.196
185.38.68.7
228.26.91.81

Domains
ytugctbfm[.]com
kcrznhnlpw[.]com
wlefihdmss.com
mbcqjsuqsd.com
humzka.com
ibfvpi.com
jiupjod.com
krlsloeohxex.com
mlvrkarzbg.com
npmuzz.com
pjhwvateyxy.com
ytugctbfm.com
ssksxalx.com
ykyru.com
HTTP Post
85.171.195.89
5.154.240.145

Mitigation and Prevention

- Use updated antimalware and antivirus, especially with real-time protection.
- Isolate infected systems and consider a full system wipe.
- Keep systems and applications patched with current updates.
- Monitor processes for alteration or injection attempts.
- Use application control software with a base deny policy.
- Compare files with known IOCs.
- Monitor systems for registry or file changes.
- Continuously monitor network traffic.

References

https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/

https://securityintelligence.com/gozi-banking-trojan-upgrades-build-to-inject-into-windows-10-edge-browser/

http://www.scmagazine.com/new-goznym-banking-malware-steals-millions-in-just-days/article/489933/

http://www.securityweek.com/hybrid-trojan-goznym-targets-north-american-banks

http://www.zdnet.com/article/goznym-the-double-headed-malware-monster-targeting-us-banks/

https://blog.team-cymru.org/2016/05/goznym-malware/

TruShield Security Solutions

TruShield is a leading provider of Managed Security Services across the globe. We are dedicated to helping companies achieve success by making sure they are properly prepared against the current and emerging threats in today's digital world. Our service offerings include: Continuous, 24/7/365 Monitoring, Penetration Testing and Vulnerability Assessments, Audit and Compliance, and many other Managed Services such as Managed Firewalls and Hosted Log Management. We also offer Security Awareness Training and Management Consulting services.
Contact us today to find out how we can help you protect your organization and safeguard your information.

Contact Information:

Email: support@trushieldinc.com
Web: www.trushieldinc.com
Phone: (877)-583-2841

Follow us on:

Twitter: @TruShield
LinkedIn: https://www.linkedin.com/company/trushield-security-solutions
Facebook: https://www.facebook.com/trushieldinc