COUNTY FARM CENTRE

Quarterly Security Report

April 1st, 2022 ——— Issue I

In this issue:

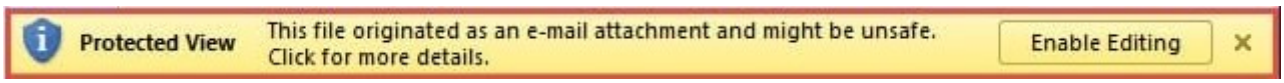
Welcome to the first issue of the County Farm Centre quarterly security report. This newsletter will cover relevant industry breaches, new malware strains, best practices for end users as well as tips and tricks for anyone looking to improving their cyber security skills.

How to analyze Malicious Microsoft Office Files

In recent years, phishing emails with malicious attachments have been one of the top vectors of compromise. A seemingly innocent Microsoft Word or Excel file could be the initial infection in a security breach. These documents often pose as receipts, bills, account information or various summary's of popular services such as Amazon accounting or Turbo Tax.

There are several ways in which Microsoft Office documents can be weaponized with malware. The most common method is a macro. A macro is a preconfigured set of instructions that can be run from a Microsoft Office document. Macros can be very useful when not employed maliciously. When weaponized, macros can be used to modify local files on a system and execute the next stage of an attack or ransomware operation.

Because of the inherent security risk with macros in Microsoft documents, Microsoft has added multiple security measures to prevent the execution of these malicious files. Protected view is what most users are familiar with. This is the yellow, warning bar that appears at the top of the document window when a user opens a file with embedded macros. Macro-enabled files end with the following extensions: .docm, .xlsm, .xlsx



If you have received a strange email from someone within your organization asking you to open a file immediately or have pressing time requirements, any emails from unknown emails, odd looking emails or just something that feels off to you. It is better to trust your instincts and reach out to your IT team or system administrator. Another option is to run the email or attachment through a virus and malware scanner. Sites like analyze.intezer.com and virustotal.com will provide a safe sandbox that will provide a clear verdict whether the file is trustworthy or malicious. These websites will also provide a detailed analysis report that will be useful in understanding the type of threat that is targeting you and your organization.

COUNTY FARM CENTRE
Quarterly Security Report
April 1st, 2022 ——— Issue I

Cyber conflict increase in Eastern Europe

Cyber conflicts are on the rise in eastern Europe as tensions between the Ukraine and Russia continue to escalate. So far we have seen three new “wiper” viruses.

The first is called HermeticWiper and it was launched just hours before ground forces moved into Ukraine. The evasive nature of HermeticWiper and its ability to bypass Windows security features have made this virus a serious threat. ESET, a Slovakian internet security company, reported a series of distributed denial-of-service (DDoS) attacks which knocked down infrastructure and several websites. This compromised systems, allowing HermecticWiper to be deployed. Following HermeticWiper are the variants CaddyWiper and IsaacWiper.

CaddyWiper has one tactical overlap with HermeticWiper in that it has been deployed to financial and governmental infrastructures by means of a Windows domain controller. This indicates that the attacks have had access to internal systems and control of active directory servers. Another common trait to recent wiper attacks is that it systematically destroys all files starting with “C:\ Users” and then moving to other drive letters. Meaning that all network drives connected to infected systems may also be affected.

These destructive attacks started on February 23rd, 2022 and have had major effects on Ukrainian websites and infrastructure. At this point, security reporting and malware defense programs have obtained samples of these malwares and are proving effective at stopping new initial infections. However, due to the current crises in Ukraine, countries and businesses that have shown support for Ukraine or sanctioned Russia; are still at risk of new attack campaigns.

Further information can be found at:

- *https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/*
- *https://www.bleepingcomputer.com/news/security/new-data-wiping-malware-used-in-destructive-attacks-on-ukraine/*

COUNTY FARM CENTRE
Quarterly Security Report
April 1st, 2022 ——— Issue I

Defense in Agriculture

The radical transformation of the agriculture industry over the past 50-years has been a remarkable feat of human innovation. Advances in sensors, devices, aerial imagery and GPS have improved profitability, efficiency and safety. Yet, these improvements come with increased risk of cyber criminals targeting these technologies.

Attacks on the agriculture sector can take wildly different forms. Everything from crop management apps, cattle tracking software, accounting software, and data backups.

Recently, three major U.S. grain distributors were infected with ransomware (which is when cybercriminals encrypt all files on a computer/network and demands payment for a key to unlock those files). This can bring entire operations grinding to a halt and in this case, it hampered their ability to process grain with any sort of efficiency. These types of attacks can affect a business of any size. Executive assistant director of the U.S Cyber Security and Infrastructure Security Agency (CISA) Eric Goldstein has said ,“Ransomware incidents can affect any organization, including small ones” [1]. Company’s of all sizes can harden there defenses by implementing these steps

Backup management: Routinely creating and restoring a copy of data that is stored both on site and in a remote location. This redundancy is important to ensuring your business can always restore the backup.

Vulnerability Assessments: Identify and qualify vulnerabilities in your network and systems. This is an analysis from the perspective of a intruder and can show the business were potential flaws lay and actions can be taken to reduce risk.

Incident response plan: The need for a detailed plan that covers incidents from network outages, data breaches, ransomware, floods, long term power outages. A detailed and thorough plan will limit the damage and facilitate a quick recovery.

[1] https://www.nbcnews.com/news/us-news/ransomware-hackers-find-vulnerable-target-us-grain-supply-rcna2702