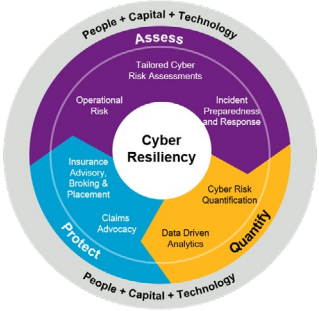


Decode cyber.

Ransomware goes mainstream as Cyber criminals open the Locker

by Jake Wingfield and Dean Chapman

Background

WastedLocker is the newest strain of ransomware being reported by cyber security organizations. First visible in May 2020, WastedLocker seems to be targeted at predominantly U.S. based organizations. Quickly attributed to a Russian cyber criminal group, it is the latest in a significant line of earlier malwares developed by Evil Corp – the group responsible for the Locky, Dridex and BitPaymer campaigns.[1]

According to recently published reports this past week, WastedLocker has claimed its most notable target to date: Garmin Ltd.[2]

What is known?

This latest attack is one of eight that targeted Fortune 500 companies this year, indeed it is believed that over 31 other large private organizations have also been attacked.[3] What Evil Corp have in store for the remaining organizations is unclear, but the threat posed has the potential for significant disruption.

In the most recent attack on Garmin (who have yet to confirm explicitly the presence of WastedLocker), initial reports point to a Taiwan facility as the point of breach.[4] This is an interesting point as it highlights the likelihood of intensive reconnaissance activity on the part of the attackers. So unlike earlier ransomware such as NotPetya, which was indiscriminate in its nature, WastedLocker (and Evil Corp) are deliberately and directly targeting firms.

Yet, if the focus of the campaign was to target U.S. companies, why is Taiwan significant? It's all about the path of least resistance. Cyber criminals, even the sophisticated ones such as Evil Corp, will always look for, the quickest and easiest 'way in'. While exact details are currently scarce, it

may be this location was perceived to have a lack of effective cyber security; alternatively it may have been identified as holding the 'Crown Jewels' and as such attracted attention as a way to gain access across the wider network. Ultimately, all the criminal group needed was a way in, targeting either technical or human 'vulnerabilities'.

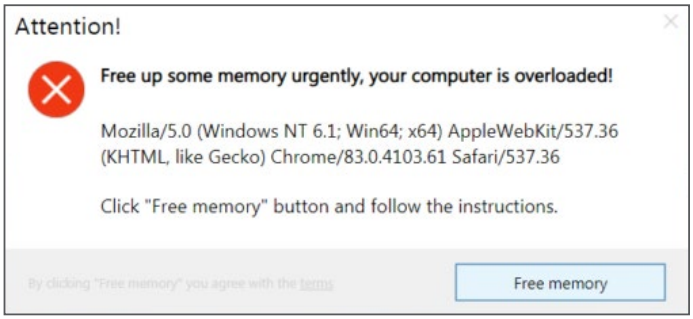
In this case, the target business has a broad range of wireless devices and applications serving five primary business units, including auto, aviation, fitness, marine and outdoor across both private and public sectors.[5] The presence of these interconnected devices on essential transportation networks raise the possibility that a cyber breach could have secondary effects on Critical National Infrastructure (CNI), as an incident at any one point in this value chain can have severe consequences in other areas.[6]

This is important because the majority of the developed world rely on Critical National Infrastructures (CNI) day in, day out. We need the communications networks to keep in touch with friends and family (especially in the current environment with the global COVID-19 crisis), transport networks to travel to work and school, and satellite networks for safe navigation and to identify the geospatial positioning of supply chains. Interruption to any of these critical services would clearly impact global economies and businesses.

Infection Method

WastedLocker follows the same path (of earlier ransomware strains from Evil Corp) and continues to play to the strengths of their highly skilled exploit and software developers, all of whom have proven themselves to be highly capable in bypassing network defences on all levels and scales.

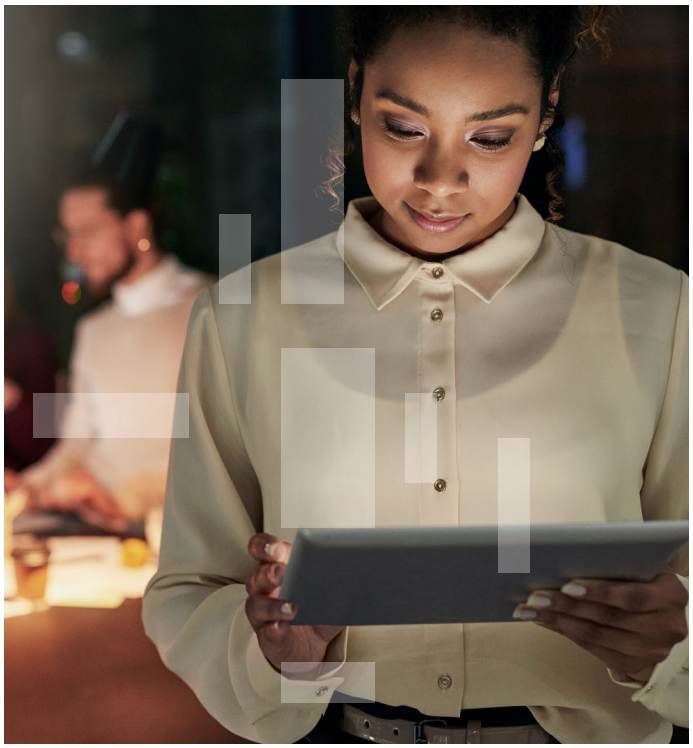
WastedLocker is named due to the filename it creates. The preferred method of infection is to utilize JavaScript to create a fake update framework, this is then used to distribute the malicious payload. The SocGholish framework is inserted into a compromised (and usually legitimate) website which results in victims seeing a very believable browser update message, similar to that presented in the image below:[7]



Source: Malwarebytes Labs

As with malicious attachments and links found within phishing emails, the intention here is to get the human to 'action' the upload – we are the path of least resistance after all...

Following the initial upload and infection, the malicious script will look to delete shadow backup files, steal credentials, escalate privileges and move laterally across the network to deploy the ransomware on as many endpoints as possible. WastedLocker doesn't actually extract or steal any data, it simply encrypts it on the host network / system before demanding payment, the extortion demand for the latest attack currently sitting at $10 million.



Geopolitical tensions

As mentioned previously, WastedLocker is the latest in a long line of highly disruptive and costly malware strains from Evil Corp. While displaying a number of similar characteristics as observed in previous ransomware, WastedLocker does indicate a slight change in Tactics, Techniques and Procedures (TTPs) by the Evil Corp group.

Evil Corp is famed for targeting file servers, databases, virtual machines (VM) and cloud environments; the impacts of their nefarious activities prompting the U.S. Treasury Department to apply sanctions and monetary fines upon the group in December 2019 (after being charged for causing more than $100 million in financial damages from 2003).[8] Considering these actions, it is probable that Evil Corp are looking to target U.S. based companies in an act of 'revenge' and to rebalance the books after significant sanctioning.

Should U.S. based firms decide to yield to ransom demands the situation may become very complex. If they pay the ransom they will potentially find themselves in violation of the United States sanction referred to above. This might prove an explanation as to why Garmin have not yet confirmed the ransoware strain to be WastedLocker, and thus Evil Corp. Non-payment could result in continued disruption and business interruption.

Working to Support our Clients

The Cyber Risk Solutions Team offers tailored services that support insurance goals, align cyber risk management with business objectives and deliver cost effective Cyber Risk Resilience. Willis Towers Watson have developed a comprehensive approach to assessing and managing the risks and impacts associated with a ransomware incident, our 3-stage methodology comprising:

Workforce Cyber Culture Assessment (WCCA)

The WCCA is an innovative assessment methodology that focuses on people and business culture, working to highlight areas of potential risk in workforce attitudes and behaviors. The analysis of findings linked to our proprietary assessment framework, as well as the identification of cyber-related cognitive biases amongst your employees, allows us to better predict the LIKELIHOOD and IMPACT of cyber security incidents, including exposure to ransomware. Effective cyber security requires a holistic approach that moves beyond just technology controls, the WCCA will support your organization in developing a 'cyber safe' workforce and culture.

Ransomware Risk Assessment (RRA)

This high-level and focused 'snapshot' of the ransomware risk(s) facing your organization is the first step towards identifying ransomware vulnerabilities. The RRA is a succinct ransomware risk report, with an easy to read executive summary, and actionable insights to aid you in improving your ransomware risk posture while reducing your threat surface. The RRA is designed to be delivered remotely in as little as 3 weeks, and our consultants will chart an easy course to guide your project sponsor through the various stages.

Cyber Risk Transfer

Cyber Risk Transfer through insurance can help companies reduce the impact of losses from ransomware. The detection of ransomware will generally trigger the cyber incident response coverage under a cyber policy, providing coverage for legal and forensics work at a minimum. To the extent the ransomware has resulted in a demonstrable interruption in the operation of the business, and loss of income could be substantiated, cyber insurance policies (and certain property policies) could also provide coverage under the business interruption insuring agreement as extra expenses incurred.

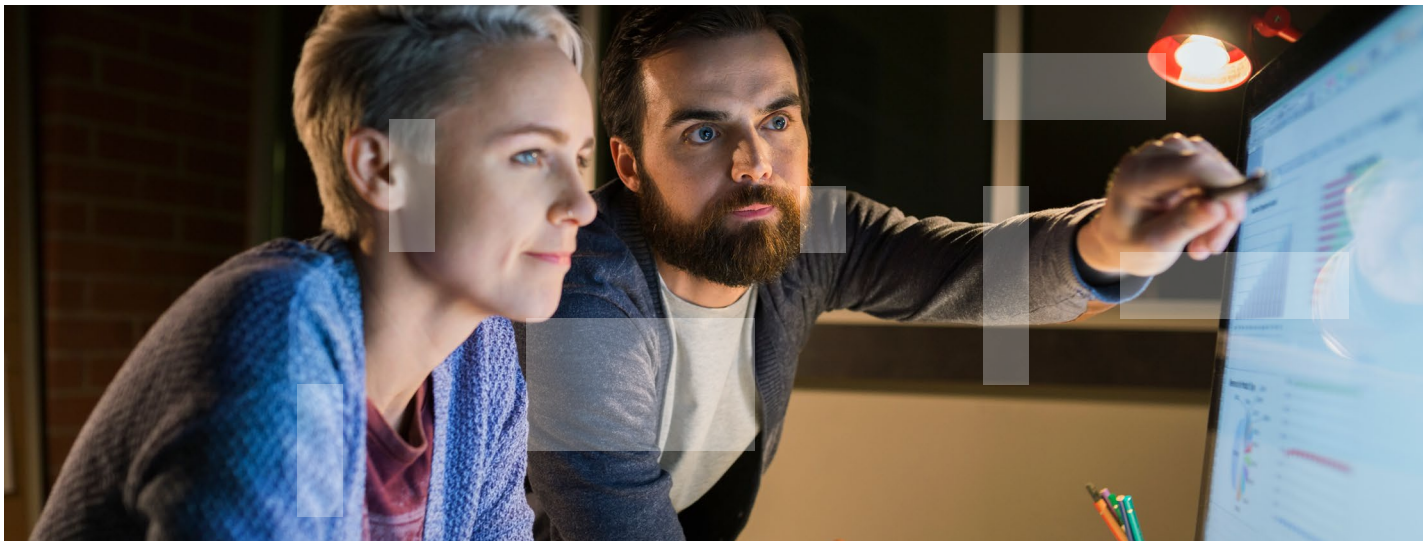
Ransomware is an ever-increasing threat and with this 'new locker open, organizations should be treating this as more than an inconvenience. A holistic, three-pronged approach involving technology, risk transfer and people-based solutions remains the optimal strategy.

For more information regarding our cyber risk services, or to discuss ransomware in greater detail with our diverse and global team of specialists, please contact:

North American Consultants:

Dominic Keller
CRS Global Team Leader
dominic.keller@willistowerswatson.com

Jonathan Davies
Cyber Risk Consultant
jonathan.davies@willistowerswatson.com



Sources

[1] https://www.cybersecurity-insiders.com/wastedlocker-ransomware-demands-10-million-as-a-ransom/

[2] https://news.sky.com/story/garmin-obtains-decryption-key-after-ransomware-attack-12036761

[3] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wastedlocker-ransomware-us

[4] https://www.zdnet.com/article/garmin-services-and-production-go-down-after-ransomware-attack/

[5] https://www.sec.gov/Archives/edgar/data/1121788/000156459020005133/grmn-10k_20191228.htm

[6] http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_Aviation_An_Industry_Analysis.pdf

[7] https://blog.malwarebytes.com/threat-spotlight/2020/07/threat-spotlight-wastedlocker-customized-ransomware/

[8] https://techcrunch.com/2020/07/25/garmin-outage-ransomware-sources/

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 45,000 employees serving more than 140 countries and markets. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

WTW475083/08/2020

willistowerswatson.com

Willis Towers Watson