They Come in the Night: Ransomware Deployment Trends

Threat Research

Kelli Vanderlee

Mar 16, 2020

7 mins read

Ransomware

Threat Research

Ransomware is a remote, digital shakedown. It is disruptive and expensive, and it affects all kinds of organizations, from cutting edge space technology firms, to the wool industry, to industrial environments. Infections have forced hospitals to turn away patients and law enforcement to drop cases against drug dealers. Ransomware operators have recently begun combining encryption with the threat of data leak and exposure in order to increase leverage against victims. There may be a silver lining, however; Mandiant Intelligence research suggests that focusing defensive efforts in key areas and acting quickly may allow organizations to stop ransomware before it is deployed.

Mandiant Intelligence examined dozens of ransomware incident response investigations from 2017 to 2019. Through this research, we identified a number of common characteristics in initial intrusion vectors, dwell time, and time of day of ransomware deployment. We also noted threat actor innovations in tactics to maximize profits (Figure 1). Incidents affected organizations across North America, Europe, Asia Pacific, and the Middle East in nearly every sector category, including financial services, chemicals and materials, legal and professional services, local government, and healthcare. We observed intrusions attributed to financially motivated groups such as FIN6, TEMP.MixMaster, and dozens of additional activity sets.

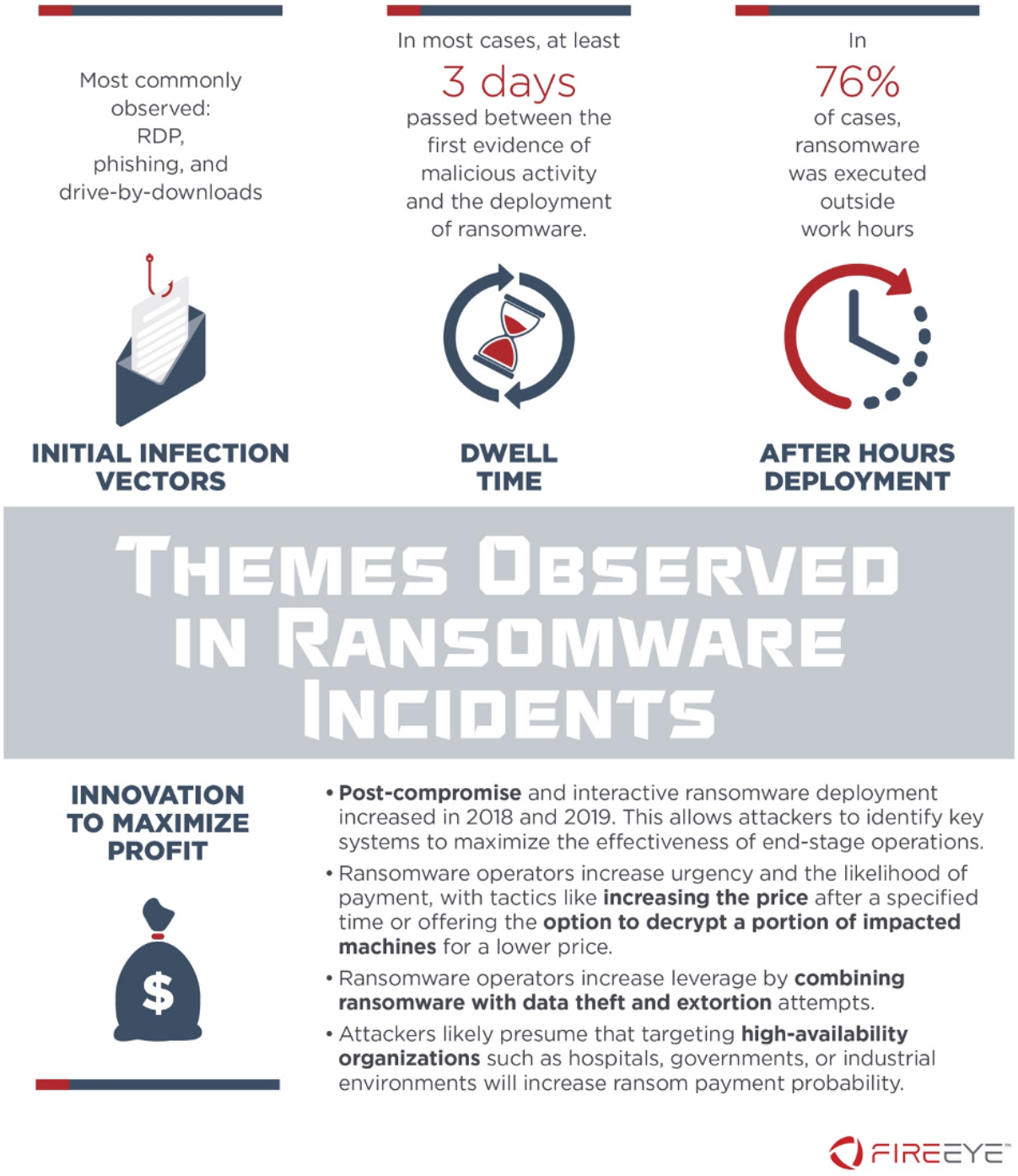

Figure 1: Themes Observed in Ransomware Incidents

These incidents provide us with enhanced insight into ransomware trends that can be useful for network defenders, but it is worth bearing in mind that this data represents only a sample of all activity. For example, Mandiant ransomware investigations increased 860% from 2017 to 2019. The majority of these incidents appeared to be post-compromise infections, and we believe that threat actors are accelerating use of tactics including post compromise deployment to increase the likelihood of ransom payment. We also observed incidents in which ransomware was executed immediately, for example GANDCRAB and GLOBEIMPOSTER incidents, but most of the intrusions examined were longer duration and more complex post-compromise deployments.

Common Initial Infection Vectors

We noted several initial infection vectors across multiple ransomware incidents, including RDP, phishing with a malicious link or attachment, and drive by download of malware facilitating follow-on activity. RDP was more frequently observed in 2017 and declined in 2018 and 2019. These vectors demonstrate that ransomware can enter victim environments by a variety of means, not all of which require user interaction.

RDP or other remote access	One of the most frequently observed vectors was an attacker logging on to a system in a victim environment via Remote Desktop Protocol (RDP). In some cases, the attacker brute forced the credentials (many failed authentication attempts followed by a successful one). In other cases, a successful RDP log on was the first evidence of malicious activity prior to a ransomware infection. It is possible that the targeted system used default or weak credentials, the attackers acquired valid credentials via other unobserved malicious activity, or the attackers purchased RDP access established by another threat actor. In April 2019, we noted that FIN6 used stolen credentials and RDP to move laterally in cases resulting in ransomware deployment.
Phishing with link or attachment	A significant number of ransomware cases were linked to phishing campaigns delivering some of the most prolific malware families in financially motivated operations: TRICKBOT, EMOTET, and FLAWEDAMMYY. In January 2019, we described TEMP.MixMaster TrickBot infections that resulted in interactive deployment of Ryuk.
Drive-by-download	Several ransomware infections were traced back to a user in the victim environment navigating to a compromised website that resulted in a DRIDEX infection. In October 2019, we documented compromised web infrastructure delivering FAKEUPDATES, then DRIDEX, and ultimately BITPAYMER or DOPPELPAYMER infections.

Most Ransomware Deployments Take Place Three or More Days After Initial Infection

The number of days elapsed between the first evidence of malicious activity and the deployment of ransomware ranged from zero to 299 days (Figure 2). That is, dwell times range quite widely, and in most cases, there was a time gap between first access and ransomware deployment. For 75 percent of incidents, at least three days passed between the first evidence of malicious activity and ransomware deployment.

This pattern suggests that for many organizations, **if initial infections are detected, contained, and remediated quickly, the significant damage and cost associated with a ransomware infection could be avoided.** In fact, in a handful of cases, Mandiant incident responders and FireEye Managed Defense contained and remediated malicious activity, likely preventing ransomware deployment. Several investigations discovered evidence of ransomware installed into victim environments but not yet successfully executed.

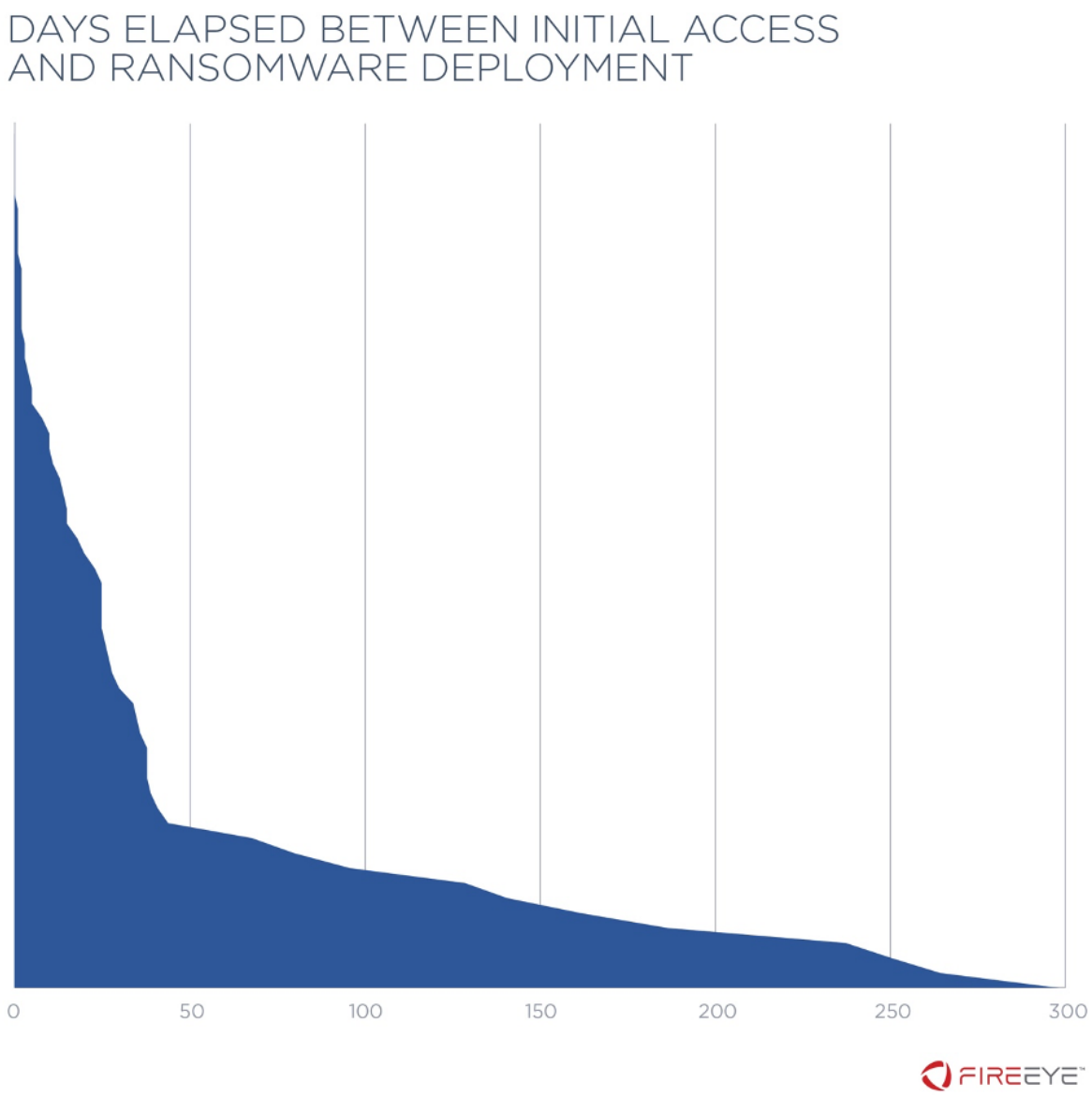

Figure 2: Days elapsed between initial access and ransomware deployment

Ransomware Deployed Most Often After Hours

In 76% of incidents we reviewed, ransomware was executed in victim environments after hours, that is, on a weekend or before 8:00 a.m. or after 6:00 p.m. on a weekday, using the time zone and customary work week of the victim organization (Figure 3 and Figure 4). This observation underscores that threat actors continue working even when most employees may not be.

Some attackers possibly intentionally deploy ransomware after hours, on weekends, or during holidays, to maximize the potential effectiveness of the operation on the assumption that any remediation efforts will be implemented more slowly than they would be during normal work hours. In other cases, attackers linked ransomware deployment to user actions.

For example, in 2019 incidents at retail and professional services firms, attackers created an Active Directory Group Policy Object to trigger ransomware execution based on user log on and log off.

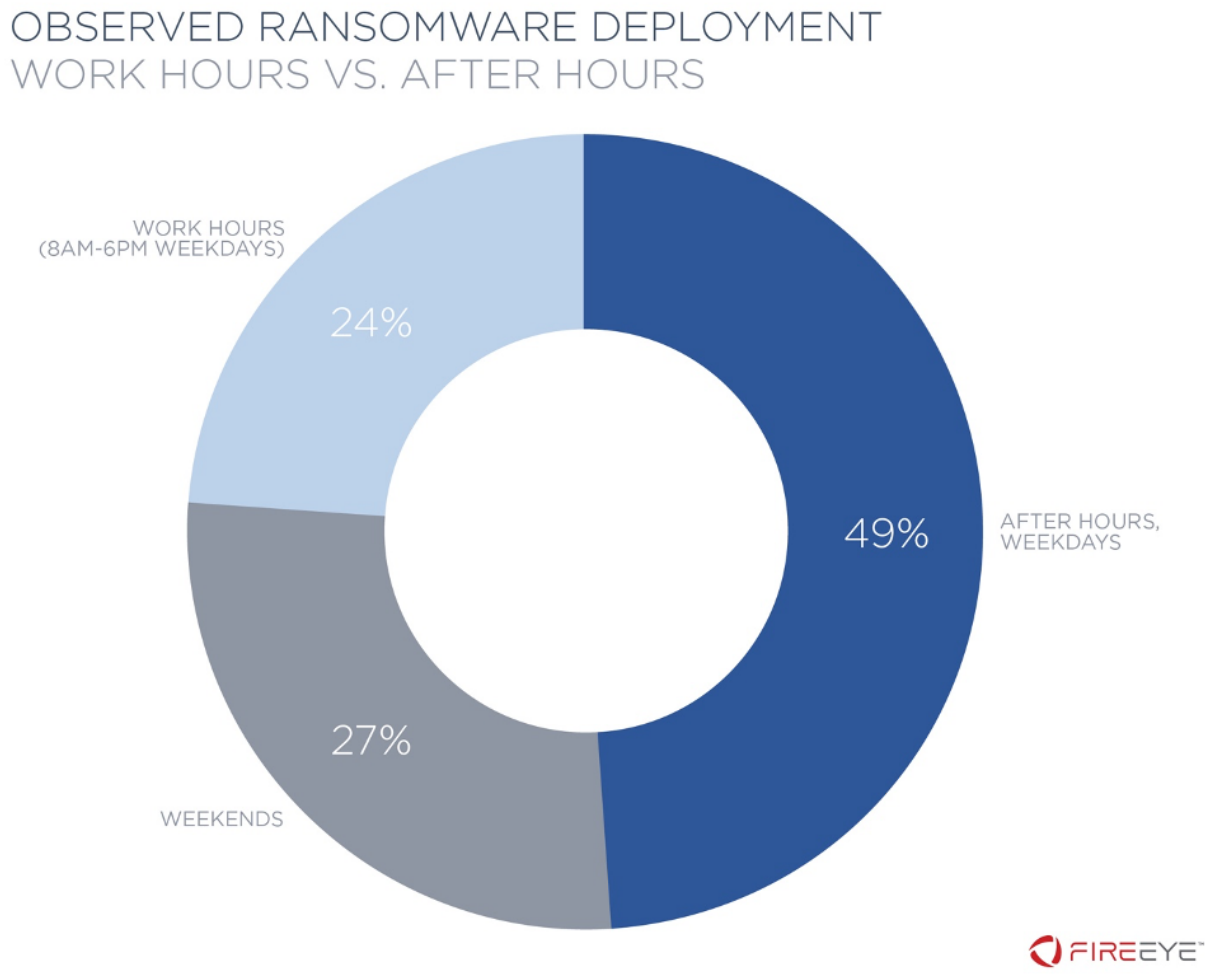

Figure 3: Ransomware execution frequently takes place after hours

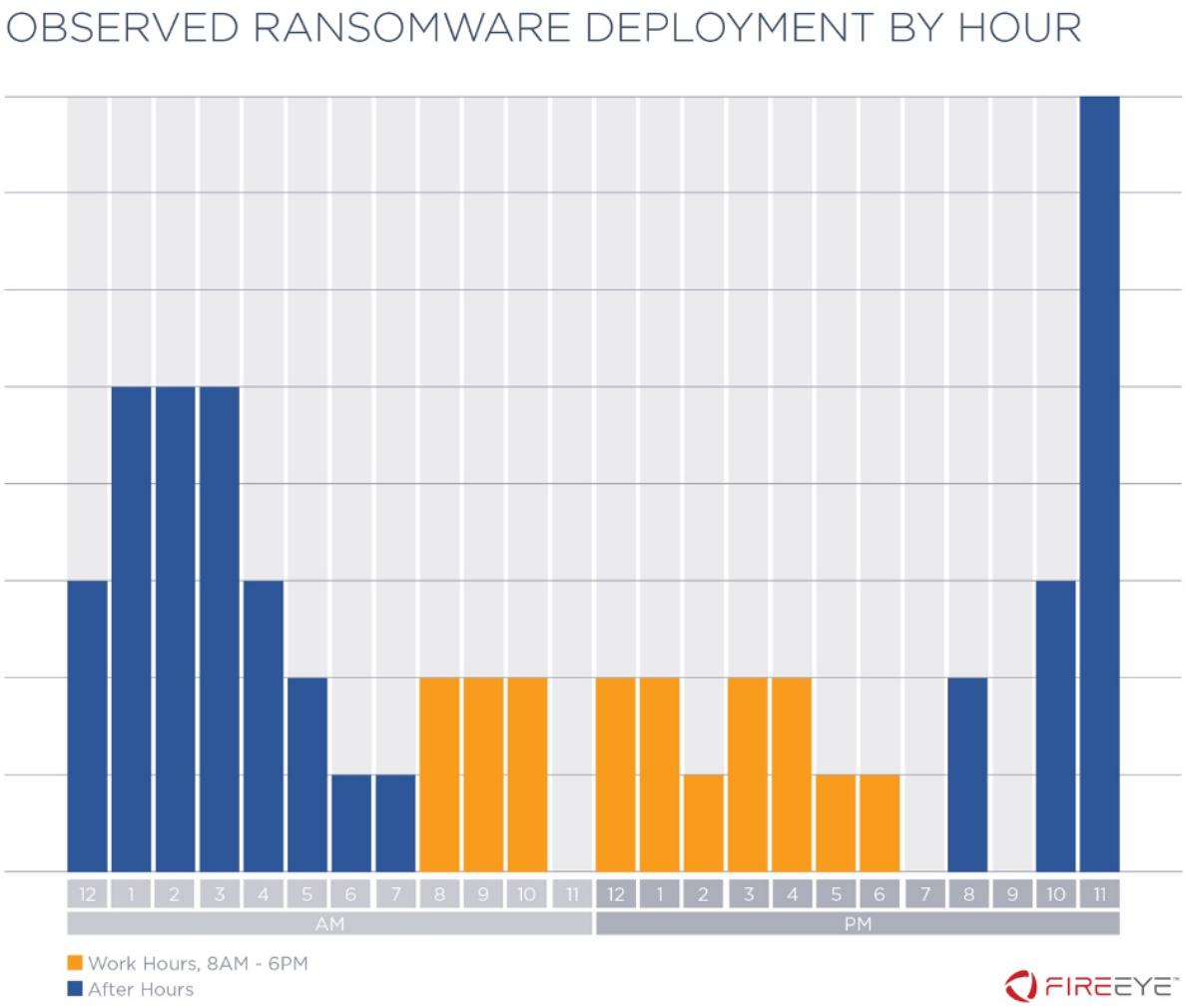

Figure 4: Ransomware execution by hour of the day

Mitigation Recommendations

Organizations seeking to prevent or mitigate the effects of ransomware infections could consider the following steps. For more comprehensive recommendations for addressing ransomware, please refer to our blog post: *Ransomware Protection and Containment Strategies: Practical Guidance for Endpoint Protection, Hardening, and Containment*.

Address Infection Vectors	• Use enterprise network, email, and host-based security products with up-to-date detections to prevent and detect many common malware strains such as TRICKBOT, DRIDEX, and EMOTET. • Contain and remediate infections quickly to prevent attackers from conducting follow-on activity or selling access to other threat actors for further exploitation. • Perform regular network perimeter and firewall rule audits to identify any systems that have inadvertently been left accessible to the internet. Disable RDP and other protocols to systems where this access is not expressly required. Enable multi-factor authentication where possible, particularly to internet-accessible connections, see pages 4-15 of the white paper for more details. • Enforce multi-factor authentication, that is, where enabled, do not allow single factor authentication for users who have not set up the multi-factor mechanism.
Implement Best Practices	• For example, carry out regular anti-phishing training for all employees that operate a device on the company network. Ensure employees are aware of threat, their role in preventing it, and the potential cost of a successful infection. • Implement network segmentation when possible to prevent a potential infection from spreading. • Create regular backups of critical data necessary to ensure business continuity and, if possible, store them offsite, as attackers often target backups. • Restrict Local Administrator accounts from specific log on types, see page 18 of the white paper for more details. • Use a solution such as LAPS to generate a unique Local Administrator password for each system. • Disallow cleartext passwords to be stored in memory in order to prevent Mimikatz credential harvesting, see p. 20 of the white paper for more details. • Consider cyber insurance that covers ransomware infection.
Establish Emergency Plans	• Ensure that after-hours coverage is available to respond within a set time period in the case of an emergency. • Institute after-hours emergency escalation plans that include redundant means to contact multiple stakeholders within the organization and 24-hour emergency contact information for any relevant third-party vendors.

Outlook

Ransomware is disruptive and costly. Threat actor innovations have only increased the potential damage of ransomware infections in recent years, and this trend shows no sign of slowing down. We expect that financially motivated actors will continue to evolve their tactics to maximize profit generated from ransomware infections. We anticipate that post-

compromise ransomware infections will continue to rise and that attackers will increasingly couple ransomware deployment with other tactics, such as data theft and extortion, increasing ransom demands, and targeting critical systems.

The good news is that particularly with post-compromise infections, there is often a window of time between the first malicious action and ransomware deployment. If network defenders can detect and remediate the initial compromise quickly, it is possible to avoid the significant damage and cost of a ransomware infection.

Register for our upcoming ransomware webinar to learn more.