A GUIDE TO LOCKERGOGA, THE RANSOMWARE CRIPPLING INDUSTRIAL FIRMS
Ransomware has long been the scourge of the cybersecurity industry. When that extortionate hacking goes beyond encrypting files to fully paralyze computers across a company, it represents not just a mere shakedown, but a crippling disruption. Now a nasty new breed of ransomware known as LockerGoga is inflicting that paralysis on industrial firms whose computers control actual physical equipment, and it's enough to deeply spook security researchers.

Since the beginning of the year, LockerGoga has hit a series of industrial and manufacturing firms with apparently catastrophic consequences: After an initial infection at the French engineering consulting firm Altran, LockerGoga last week slammed Norwegian aluminum manufacturer Norsk Hydro, forcing some of the company's aluminum plants to switch to manual operations. Two more manufacturing companies, Hexion and Momentive, have been hit by LockerGoga—in Momentive's case leading to a "global IT outage," according to a report Friday by Motherboard. And incident responders at security firm FireEye tell WIRED they've dealt with multiple LockerGoga attacks on other industrial and manufacturing targets they declined to name, which would put the total number of victims in that sector at five or more.

Security researchers also say that the most recently discovered strain of the malware is particularly disruptive, shutting down computers entirely, locking out their users, and rendering it difficult for victims to even pay the ransom. The result is a dangerous combination: reckless hacking that...
targets a set of companies that are highly incentivized to quickly pay the ransom, but also ones where a cyberattack could wind up physically harming equipment or even a factory's staff.

"If you cripple the ability to operate an industrial environment, you’re costing that enterprise significant amounts of money and really applying pressure for every minute that loss of control continues," says Joe Slowik, a researcher at the security firm Dragos, which focuses on industrial control systems. "Unless that system is in a steady state of operation or has good physical fail-safes, you now have a process out of your control and out of view of your own eyes. That makes this extremely irresponsible and very nasty."

Anatomy of an Extortion

LockerGoga, which was named for a file path in its source code by security research group MalwareHunterTeam, remains relatively rare and targeted compared with older forms of ransomware like SamSam and Ryuk, says Charles Carmakal, who leads a team of incident responders at FireEye that has dealt with multiple infestations. FireEye, for instance, has seen fewer than 10 victims, though MalwareHunterTeam estimates the total victim count in the dozens. It's not clear how the LockerGoga hackers are gaining initial access to victim networks in those targeted cases, but Carmakal has found that they seem to already know targets' credentials at the start of an intrusion, perhaps thanks to phishing attacks or by simply buying them from other hackers. Once the intruders have an initial foothold, they use the common hacking toolkits Metasploit and Cobalt Strike to move to other computers on the network and also exploit the program Mimikatz, which can pull traces of passwords out of the memory of Windows machines and allow them to gain access to more privileged accounts.

After they obtain a network's highest privilege "domain admin"
credentials, they use Microsoft's Active Directory management tools to plant their ransomware payload on target machines across the victim's systems. That code, Carmakal says, is signed with stolen certificates that make it look more legitimate. And before running their encryption code, the hackers use a "task kill" command on target machines to disable their antivirus. Both of those measures have made antivirus particularly ineffective against the subsequent infections, he says. LockerGoga then rapidly encrypts the computer's files. "On an average system within a few minutes, it is toast," wrote Kevin Beaumont, a UK security researcher, in an analysis of the Norsk Hydro attack.

Finally, the hackers plant a readme file on the machine that lists their demands. "Greetings! There was a significant flaw in the security system of your company," it reads. "You should be thankful the flaw was exploited by serious people and not by some rookies. They would have damaged all your data by mistake or for fun." The note doesn't name a ransom price but instead provides email addresses, demanding the victim contact the hackers there to negotiate a bitcoin sum for the return of their systems, which according to FireEye are typically in the hundreds of thousands of dollars.

Cruel and Unusual Punishment

In the latest version of the malware that researchers have analyzed, LockerGoga goes further still: It also disables the computer's network adapter to disconnect it from the network, changes the user and admin passwords on the computer, and logs the machine off. Security researchers have found that in some cases, the victim can log back in with a particular password, "HuHuHUHoHo283283@dJD," or with a cached domain password. But the result, even so, is that unlike more typical ransomware, the victim often can't even see the ransom message. In some cases, they may not even know that they've been hit with
ransomware, delaying their ability to recover their systems or pay the extortionists, and causing even greater disruptions to their network.

That's a very different approach from typical ransomware that merely encrypts some files on a machine but otherwise leaves it running, says Earl Carter, a researcher at Cisco's Talos division. The degree of disruption is counterproductive even for the hackers, since they're less likely to be paid, he argues. "Everyone is kicked off the system so they can't even get back to look at the ransom note," he says. "It throws everything into chaos. You've just destroyed the operation of the system, so users can't do anything at all, which is a much more significant impact on the network" than a typical ransomware attack.

But FireEye's Carmakal insists that the LockerGoga hackers are nonetheless profit-focused, and not merely seeking to sow chaos. He says some victims have in fact paid six-figure ransoms and had their files returned. "Quite frankly I question whether it's a deliberate design by the threat actor," Carmakal adds. "Did they understand the consequences of how much more difficult it would be? Or did they want it this way? I really don't know."

Industrial-Level Pain

FireEye notes that LockerGoga's victims aren't limited to industrial or manufacturing victims. Instead, the victims include "targets of
Meet LockerGoga, the Ransomware Crippling Industrial Firms | WIRED

opportunity” in other business sectors too—any company that hackers believe will pay and for which they can gain an initial foothold. But the unusual number of crippled industrial firms LockerGoga has left in its wake, combined with its hyperaggressive effects, represent an especially serious risk, according to Dragos’ Joe Slowik.

Slowik warns that the more recent, disruptive form of the malware could easily infect the computers those firms use to control industrial equipment—the so-called "human-machine interface" or HMI machines that run software sold by companies like Siemens and GE for remotely managing automated physical processes. In the worst-case scenario, the ransomware might paralyze those computers and lead to unsafe conditions or even industrial accidents.

"Doing something as indiscriminate and as thoroughly disruptive as what LockerGoga can do on industrial control devices is not good," says Slowik. "You typically don't test these systems in a situation where your ability to control or monitor them is taken away from you. If anything changes, you're unable to react to it, and any situation that develops can become a crisis very quickly."

One disturbing example of that nightmare scenario was a case that came to light in 2014 when a German steel mill was hit by unknown hackers. The attack, whether intentionally or not, prevented the plant’s operators from shutting down a blast furnace, causing "massive damage," according to a German government report on the incident, which didn't name the company involved.

That sort of catastrophe, to be clear, is only a troubling edge case, Slowik notes. It's not yet clear if LockerGoga infected any of the industrial control systems of victims like Hexion, Norsk Hydro, or Momentive, rather than their traditional business IT networks. And even if it did infect those control systems, Slowik points out that industrial facilities implement both independent digital protections
—such as safety-instrumented systems that monitor unsafe conditions in a plant—and physical fail-safes that could prevent a dangerous accident.

But even so, if those sorts of fail-safes became necessary, they would still likely cause an emergency shutdown that itself would represent a serious, costly disruption for an industrial hacking victim—likely one that's even worse than the kind LockerGoga's industrial victims are already facing. "Nothing might have blown up, but it's not a trivial impact," Slowik says. "You're still left with a situation where your plant is shut down, you have a significant recovery operation ahead of you, and you’re losing money by the minute. The company is still in a world of hurt."

More Great WIRED Stories

- Airbnb’s “guerrilla war” against local governments
- Change your Facebook password right now
- With Stadia, Google's gaming dreams head for the cloud
- A more humane livestock industry, thanks to Crispr
- For gig workers, client interactions can get ... weird
- 🕹️ Looking for the latest gadgets? Check out our latest buying guides and best deals all year round
- 🕹️ Get even more of our inside scoops with our weekly Backchannel newsletter

When you buy something using the retail links in our stories, we