# Leading U.S. laser developer IPG Photonics hit with ransomware

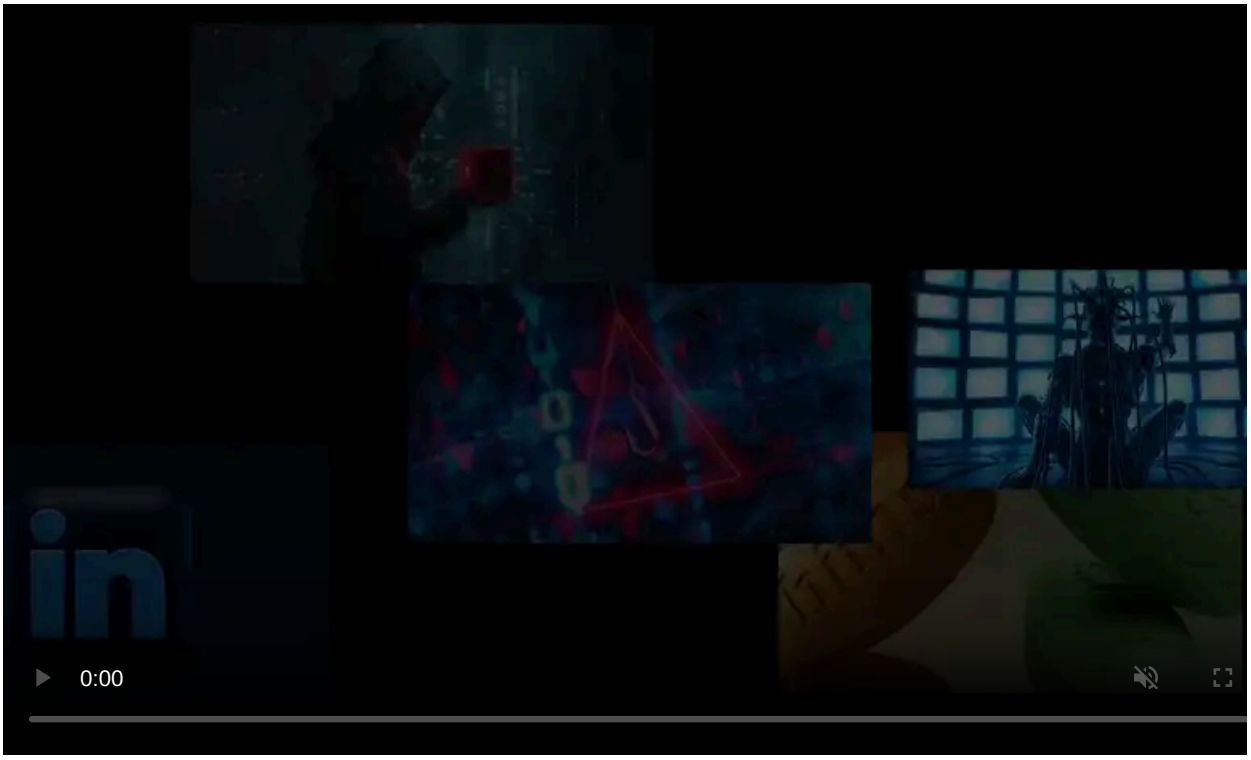
By Lawrence Abrams

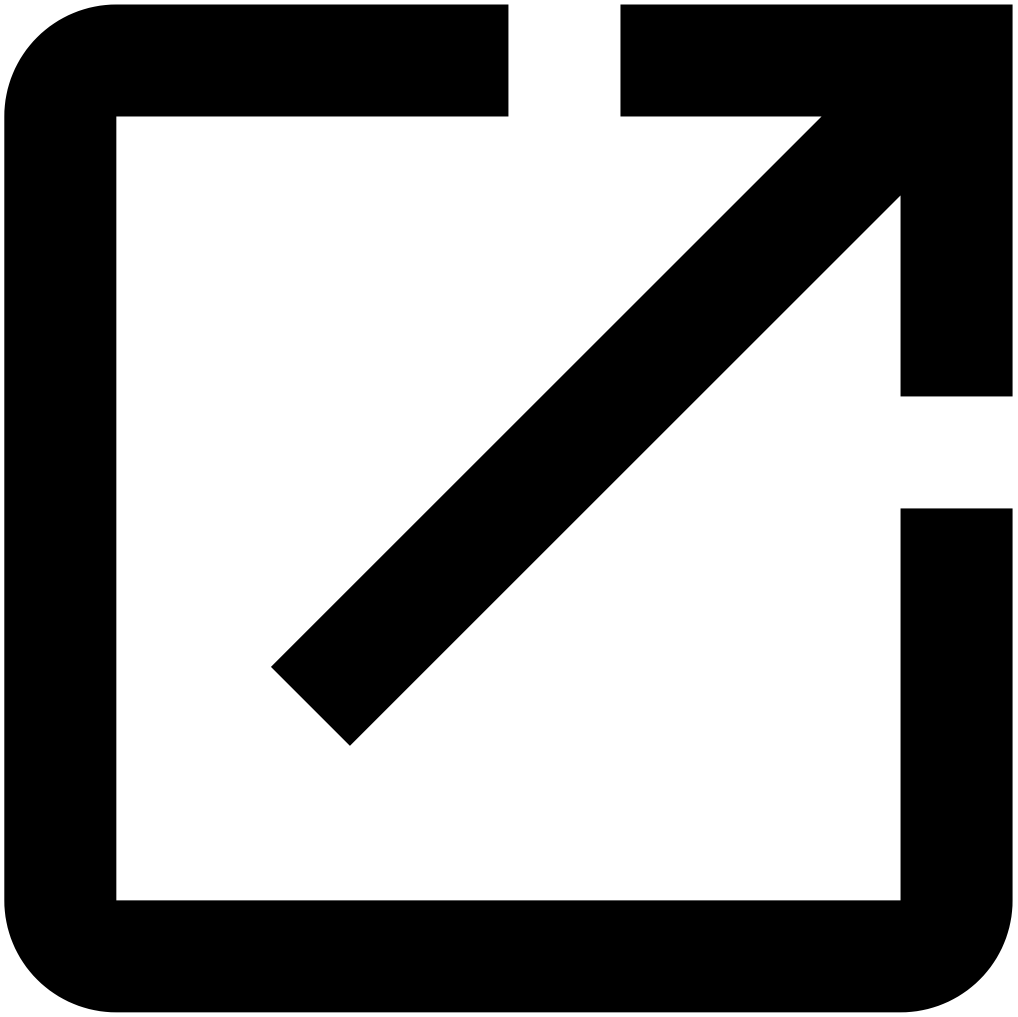
Published: 2020-09-18 · Archived: 2026-04-05 16:52:18 UTC

IPG Photonics, a leading U.S. developer of fiber lasers for cutting, welding, medical use, and laser weaponry has suffered a ransomware attack that is disrupting their operations.

Based out of Oxford, Massachusets, IPG Photonics has locations worldwide where they employ over 4,000 people and have a $1.3 billion revenue in 2019.

The company's lasers were used as part of the U.S. Navy's Laser Weapon System (LaWS) that was installed on the USS Ponce. This system is an experimental defensive weapon against small threats and vehicles.


0:00



## IPG Photonics disrupted by a ransomware attack

On Monday, BleepingComputer was contacted by a source with knowledge of the attack who told us that a ransomware attack had disrupted its operations.

Due to the attack, IPG Photonics IT systems are shutdown worldwide, affecting email, phones, and network connectivity in the offices.

With these systems down, BleepingComputer is also being told that manufacturing parts and shipping have become unavailable.

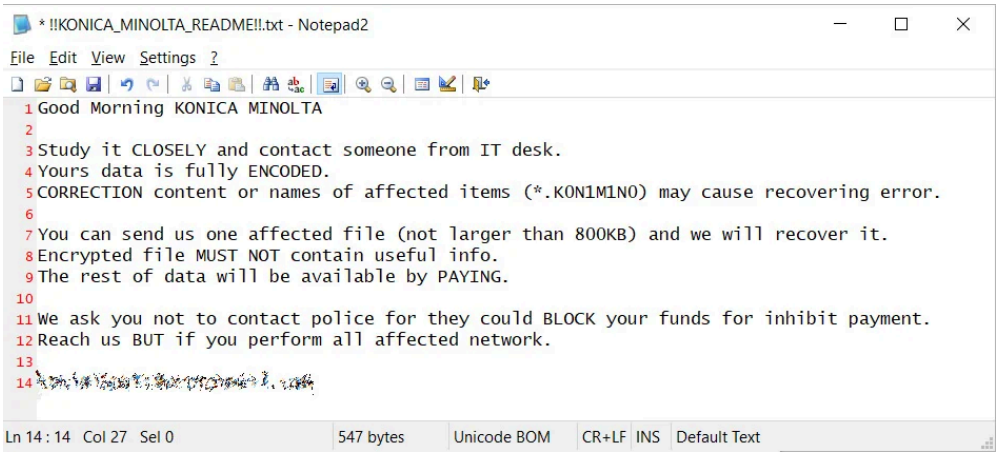
If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at +16469613731.

A partial ransom note seen by BleepingComputer also indicates that the RansomExx ransomware operation conducted the attack.

RansomExx is a rebranded version of the Defray777 ransomware and has seen increased activity since June when they attacked the Texas Department of Transportation (TxDOT) and Konica Minolta in August.

Like other RansomExx ransom notes, the attackers tell the victim not to contact law enforcement as ransom payments could be blocked.

This same message is shown in the ransom note left behind during the Konica Minolta Ransomware attack.

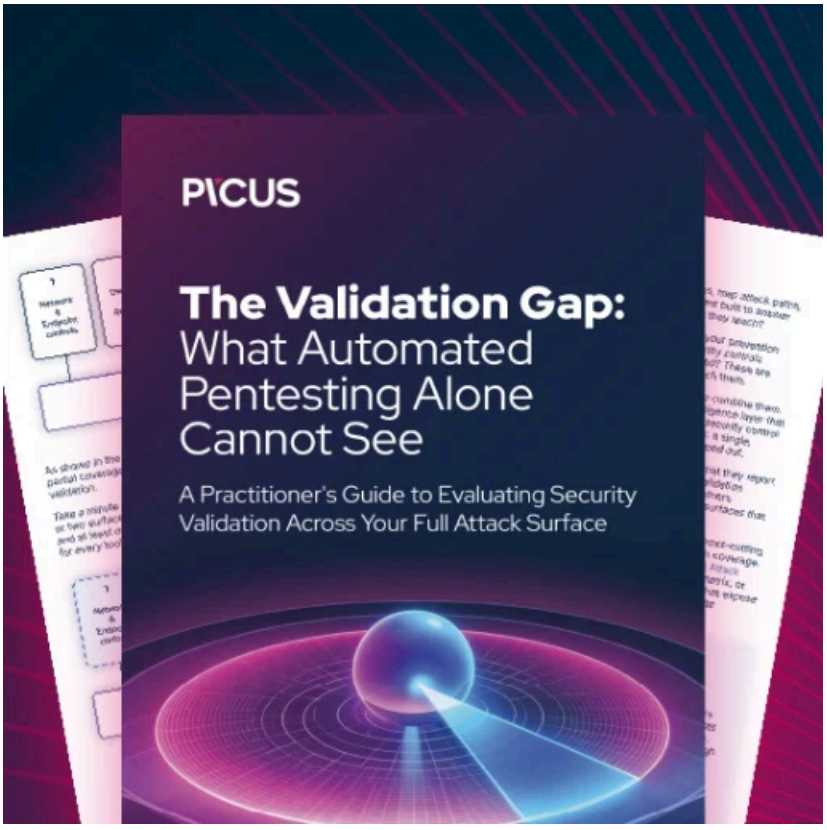



**Konica Minolta ransom note**

The ransom note also claims that the attackers have stolen data from "TFS repositories and something else."

Ransom EXX does not have a ransomware data leak site, and we are not aware of them releasing victim's stolen data in the past.

BleepingComputer has emailed and called IPG Photonics repeatedly for comment but has not received replies as of yet.




## Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---

Source: https://www.bleepingcomputer.com/news/security/leading-us-laser-developer-ipg-photonics-hit-with-ransomware/