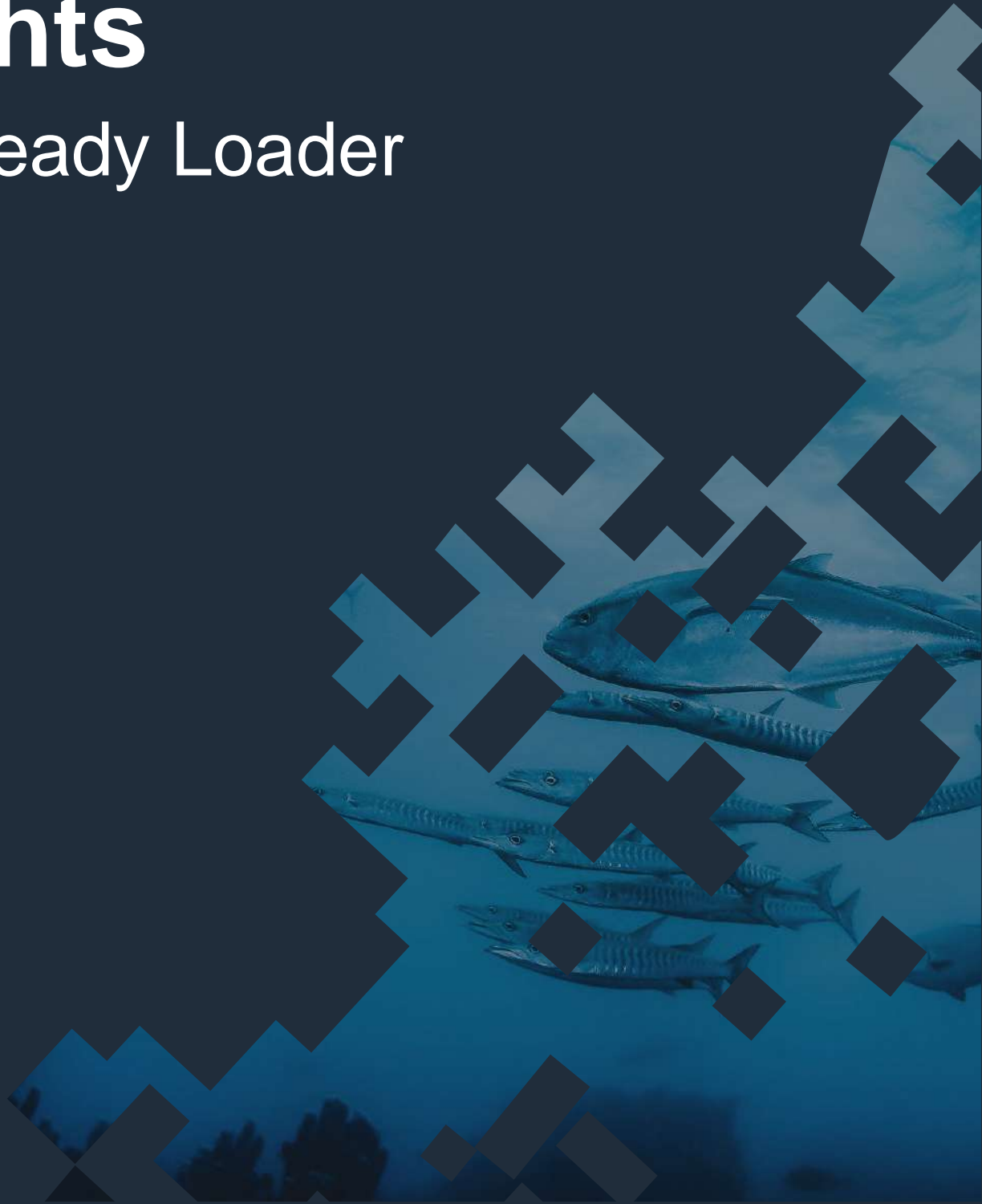


Threat Intelligence Insights

| SVCReady Loader



A Malicious Spam Campaign Targeting **European Countries**

In April 2022, the PRODAFT Threat Intelligence (PTI) team detected a malicious loader called SVCReady. The loader is heavily distributed through phishing campaigns.

The malicious spam (malspam) campaign features an unusual way of loading the malware from Word documents onto compromised devices.

The SVCReady loader is actively being developed, with frequent functionality updates to strengthen its capabilities. Our PTI team is tracking new victims as they are added.

Attack Highlights

Threat Type:
Botnet




Resource Level:
Organized team



Main Targets:
**Italy, France,
and Ukraine**



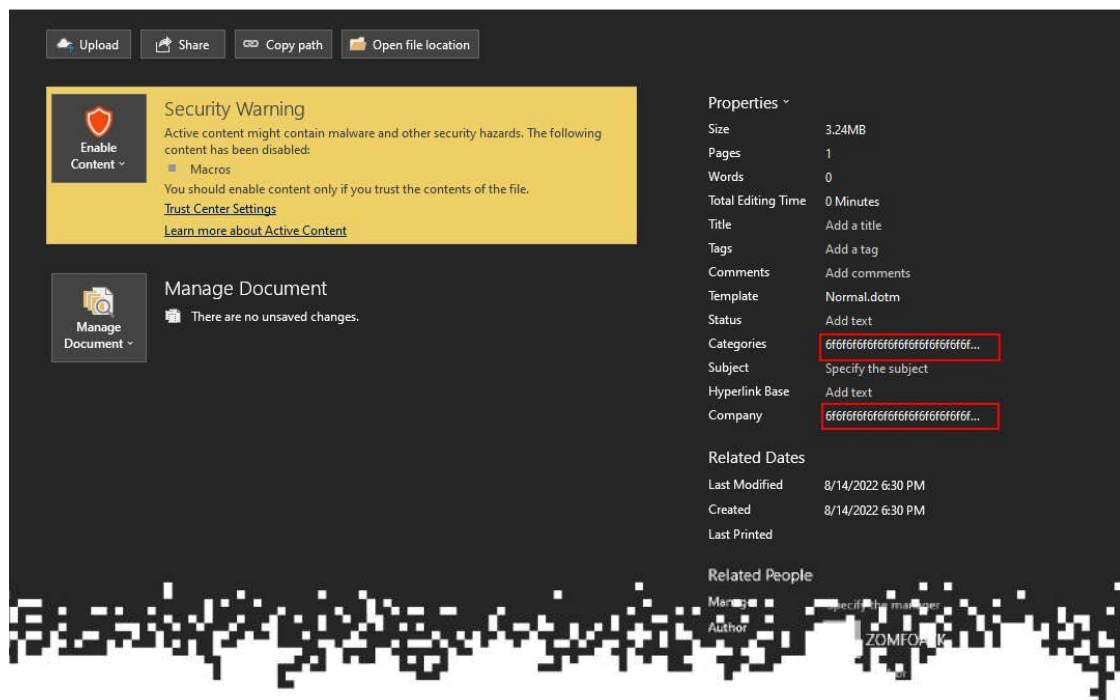
Primary Motivation:
Personal gain



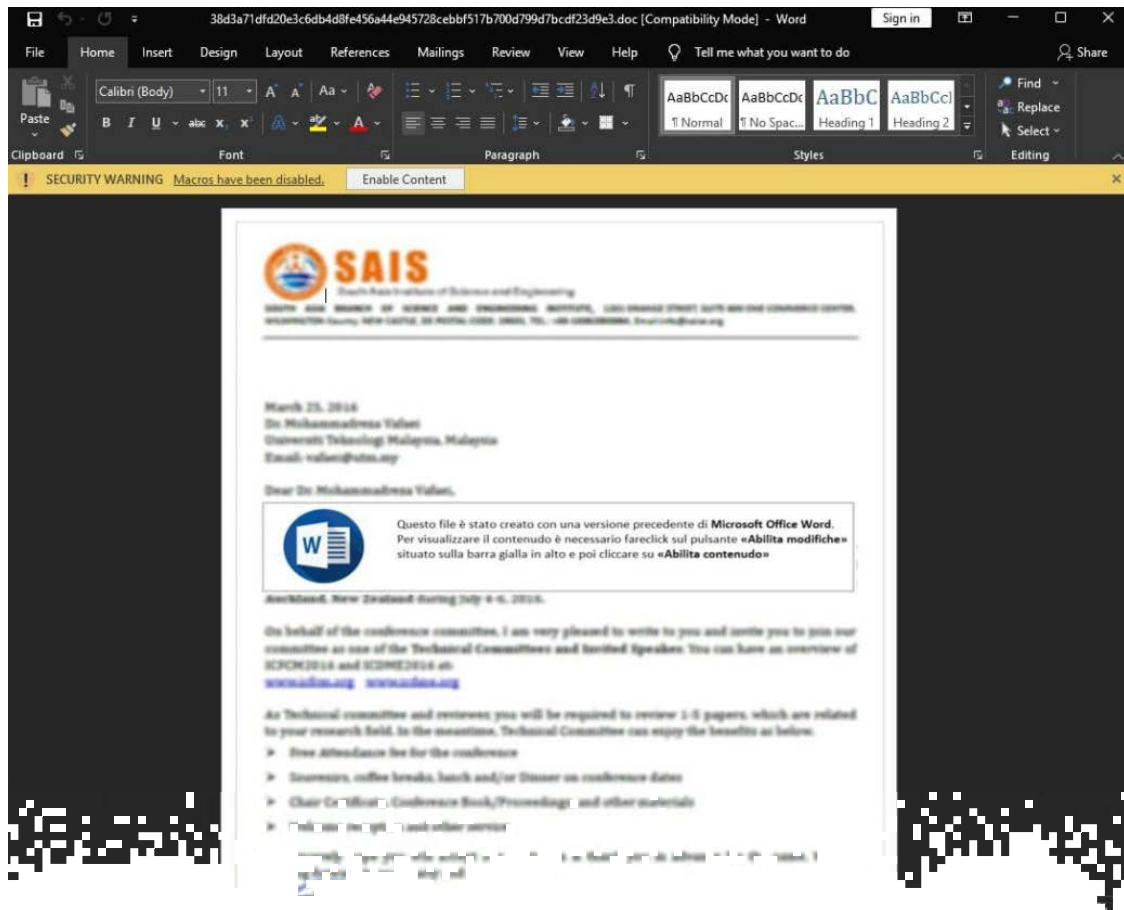
The Strategy

The phishing emails include an MS Word attachment containing a malicious Macro script. Macros are executable scripts embedded in MS Office documents to automate tasks but can also be used maliciously by attackers.

This infection method has been well-known for many years, but if well-prepared, it can still avoid detection from many AV/EDR solutions.



The sample Word documents show the threat actors kindly asking the victims to enable Macro to view the blurred content. We found that the documents are prepared in many languages, depending on the targeted countries.



Once the device is compromised, the malware can perform a long list of actions, including running shell commands, taking screenshots, and downloading files to the compromised device.

The Attacker

We discovered that SVCReady loader has considerable overlap in tactics with TA551 and TA505. However, the exact attribution of the campaigns is unclear for now.

The Findings

According to our findings, the threat actors target corporate companies, government institutions, and educational and financial entities. The number of devices that belong to home users is low. Currently, there are 25'850 victims, including 4 U.S.T.A. customers.



The U.S.T.A. platform ensures detection and takedown of all phishing threats without requiring additional requests or interactions.

Our platform is reinforced with various detection mechanisms (based on keyword, structure, image, and other similarities) that monitor the cyber-world to discover phishing websites targeting U.S.T.A. member organizations.

Our clients are guaranteed to be protected against all potential, expected, or active phishing threats. We're constantly challenging ourselves to think one step ahead and design new detection technologies for future evasion techniques.