Security Brief: TA551 Uses ‘SLIVER’ Red Team Tool in New Activity

proofpoint.com/us/blog/security-briefs/ta551-uses-sliver-red-team-tool-new-activity

October 20, 2021

Blog
Threat Insight
Security Brief: TA551 Uses ‘SLIVER’ Red Team Tool in New Activity

October 20, 2021 BRYAN CAMPBELL, SELENA LARSON AND THE PROOFPOINT THREAT INSIGHT TEAM

Proofpoint researchers identified a new campaign from the highly active cybercrime actor known as TA551 using a legitimate “Red Team & adversary simulation Framework”. The new activity demonstrates a significant departure from the previously observed activity from this group. Proofpoint assesses with high confidence the new activity could lead to ransomware infections.

TA551 is a criminal threat actor Proofpoint has tracked since 2016. It is known by other security firms as Shathak. Proofpoint assesses with high confidence TA551 gains access to stolen messages or compromised email accounts – also known as thread hijacking – which it uses in email campaigns to distribute malware. TA551 has previously distributed malware payloads such as Ursnif, IcedID, Qbot, and Emotet. This actor acts as an initial access facilitator for ransomware threat actors. Proofpoint has observed its campaigns leveraging banking trojans have led to ransomware infections. Proofpoint assesses with high confidence TA551 IcedID implants were associated with Maze and Egregor ransomware events in 2020.

On 20 October 2021, Proofpoint observed emails that appeared to be replies to previous conversations and contained password-protected zipped Word documents. The attachments ultimately lead to the download of Sliver, an open-source, cross-platform adversary simulation and red team platform. The activity demonstrated a significant departure from previous tactics, techniques, and procedures from TA551.

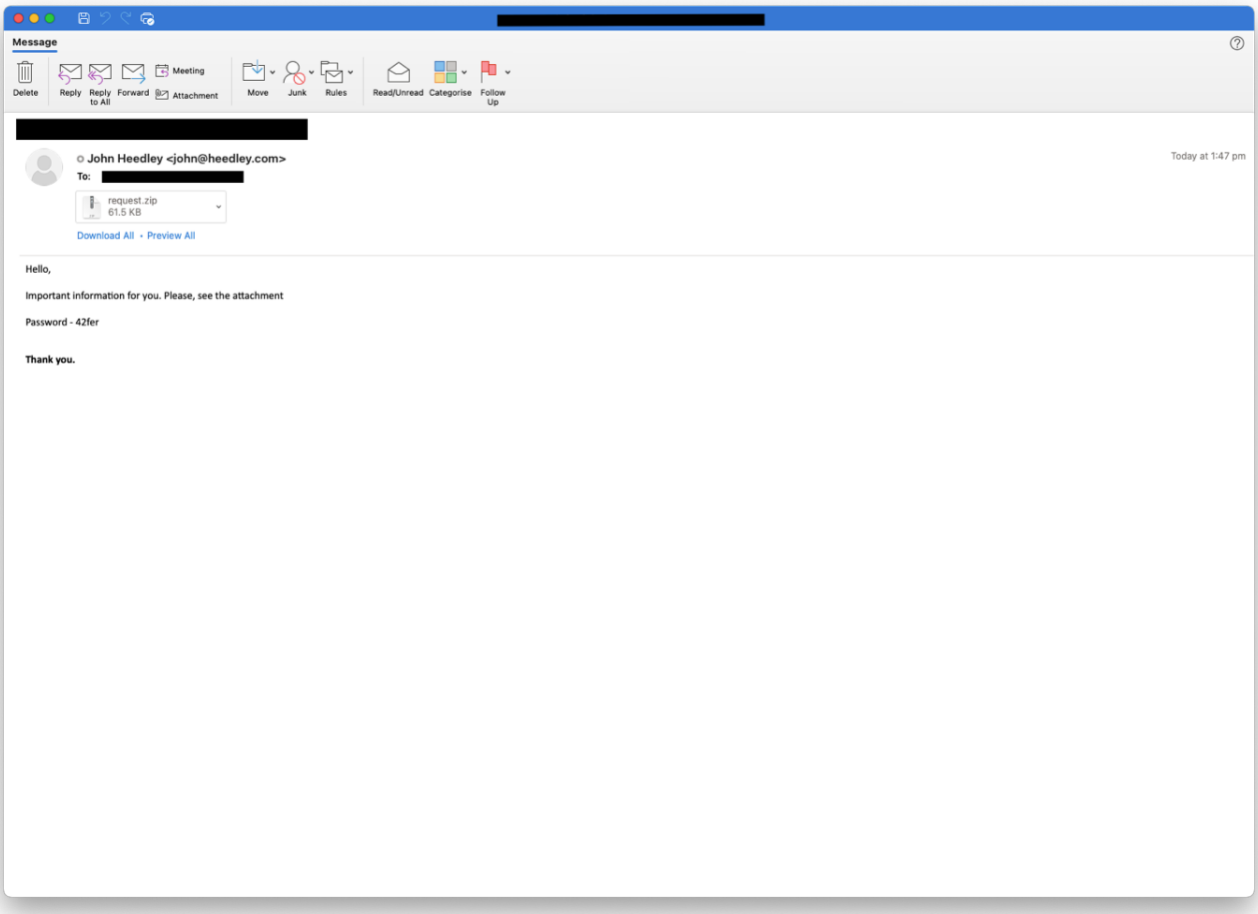

Figure: Thread hijacked email containing zipped Word document.

When a victim downloads the zipped attachment, they are ultimately directed to a macro-laden Microsoft Word document. If macros are enabled, SLIVER is downloaded.

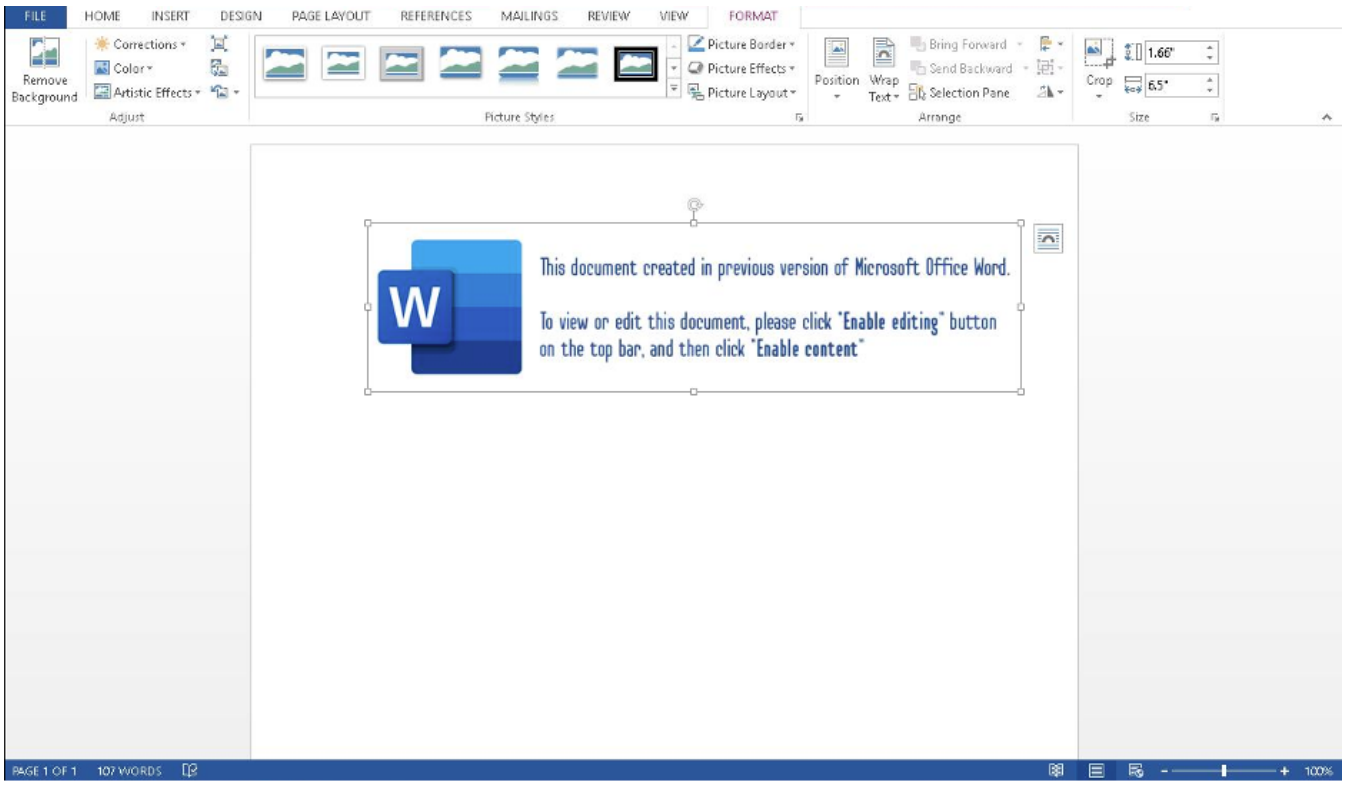

Figure: Malicious Microsoft Word document directing victims to enable macros.

SLIVER is available for free online, and capabilities include information gathering, command and control (C2) functionality, token manipulation, process injection, and other features. Red teaming tools are becoming increasingly popular with cybercrime threat actors. For instance, Proofpoint observed a 161% increase in threat actor use of the red teaming tool Cobalt Strike between 2019 and 2020. Additional offensive frameworks that appear as first stage payloads used by cybercrime actors include Lemon Tree and Veil.

TA551's use of SLIVER demonstrates considerable actor flexibility. As an established initial access broker leveraging initial access via email threat campaigns, TA551 would compromise a victim and potentially broker access to enable the deployment of Cobalt Strike and eventually ransomware. With SLIVER, TA551 actors can gain direct access and interact with victims immediately, with more direct capabilities for execution, persistence, and lateral movement. This potentially removes the reliance on secondary access.

Proofpoint observed the following indicators of compromise:

Indicator	Description
hXXp://carwaded[.]com/cbfsd/P9G7gD1E6t9w22zQj/cC9DHcTHUKJV/ugnbvdk0EInGgeCqaLEYILzxL/zes1?ref=wU4bJ1ZLhoMc8BcRMMqy&q=ELOKZymM	Document Payload
hXXp://ruwejo[.]com/upload/admin.jsp	SLIVER C2
b7cc07bfc41e61a89e961dd5826fa2b4d47a85a5b5856d50f9a57667199635b3	Document SHA256

Emerging Threats Signature

ETPRO MALWARE Sliver Framework HTTP C2 sessionInit

Is your organization protected against criminal threat actors? Learn about Ransomware attacks and prevention.

Subscribe to the Proofpoint Blog