НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

# Об использовании злоумышленниками легитимных RAT-инструментов

ALRT-20211122.1 |22 ноября 2021 г.

Уровень угрозы: ВЫСОКИЙ

TLP: WHITE

| | |
|---|---|
| Актуальность угрозы | Актуально по настоящее время |
| Описание | По каналам Национального координационного центра по компьютерным инцидентам получены сведения об активном использовании злоумышленниками легитимных инструментов удаленного администрирования (Remote Administration Tool) в рамках осуществления различной вредоносной деятельности.<br>Remote Administration Tool, известные также как RAT-инструменты, в большинстве случаев используются системными администраторами для получения удаленного доступа к элементам ИТС организации. Среди отличительных особенностей таких инструментов возможно выделить удобный интерфейс управления и отсутствие необходимости в настройке пограничных межсетевых экранов для последующего доступа к ресурсам.<br>Большинство RAT-инструментов функционирует по принципу клиент-сервер. Таким образом соединение устанавливается со стороны управляемого в ИТС организации ресурса к удаленным серверам администратора или к серверам-посредникам, которые находятся в распоряжении производителей программного обеспечения.<br>С точки зрения злоумышленника такие особенности функционирования RAT-инструментов позволяют ему скрыть свое присутствие в ИТС организации под видом легитимной деятельности системных администраторов и не требуют проведения дополнительных мероприятий для создания канала удаленного управления.<br>Внедрение RAT-инструментов в ИТС организации может осуществляться злоумышленником как на этапах доставки модулей вредоносного программного обеспечения посредством целенаправленной фишинговой рассылки, так и любым другим возможным для него способом.<br>В результате внедрения в ИТС организации RAT-инструментов злоумышленник получает в свое распоряжение полнофункциональное средство удаленного управления скомпрометированной операционной системой, функционирование которого не детектируется стандартными средствами защиты информации как вредоносное событие. |

В качестве мер противодействия данной угрозе НКЦКИ рекомендует оценить необходимость использования данных средств в ИТС организации. В случае отсутствия такой необходимости рекомендуем заблокировать возможность обращения к IP-адресам и доменным именам, входящим в инфраструктуру наиболее распространенных RAT-инструментов.

В случае последующего выявления попыток обращения к заблокированным ресурсам, необходимо провести мероприятия по установлению их источников и возможной связи с активностью вредоносного программного обеспечения

Перечень индикаторов рекомендуемых к блокированию

| Название средств удаленного администрирования | Список используемых доменных имен и IP-адресов |
|---|---|
| TeamViewer | master*.teamviewer.com<br>*.dyngate.com |
| Ammyy Admin | rl.ammyy.com |
| Radmin | radmin.ru<br>radmin.com |
| Remote Manipulator System | rmansys.ru |
| AnyDesk | relays.net.anydesk.com<br>*.anydesk.com |
| LiteManager | litemanager.ru<br>89.108.101.61<br>91.240.86.200 |
| AeroAdmin | aeroadmin.com<br>auth*.aeroadmin.com |