КОД безопасности

Новый вид хакерских атак в условиях удаленной работы

Фёдор Дбар
Коммерческий директор

КОД безопасности

План

- Перспективы удаленной работы
- Примеры рисков ИБ
- Возможные решения

Что нас ждет

01 Гибридная форма работы

02 Минимум до 2024 года

03 Доля удалённщиков до 60%

01/31/2021

Gartner

Forecast Analysis: Remote Workers Forecast, Worldwide

Published 21 August 2020 - ID G00727672 - 20 min read

By Analysts Ranjit Atwal, Anna Griffen, Rishi Padhi, Namrata Banerjee

Initiatives: Technology Market Essentials

The impact of COVID-19 has made remote working a necessity. Employers must create a hybrid workplace that balances employees' needs with business success. By 2024, remote workers will represent 30% of all employees worldwide, an increase of 13% over 2019, to nearly 600 million employees.

Forecast Assumptions

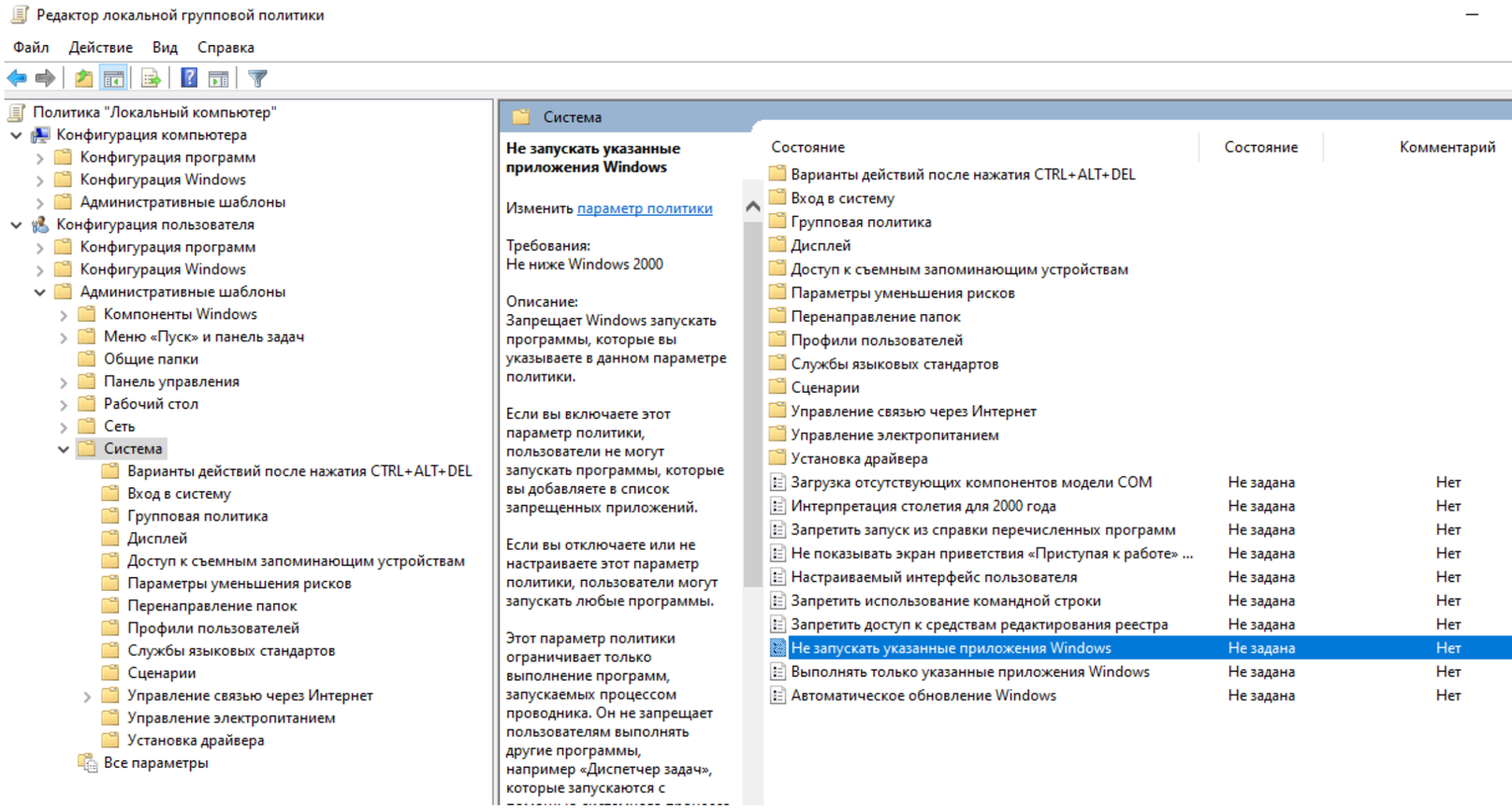
- Social distancing will be a reality throughout 2021.
- Through 2024, around 30% of all employees working remotely will permanently work at home.
- By the end of 2024, the change in the nature of work will increase the total available remote worker market to 60% of all employees, up from 52% in 2020.
- By 2024, in-person meetings will drop from 60% of enterprise meetings to 25%, driven by remote work and changing workforce demographics.

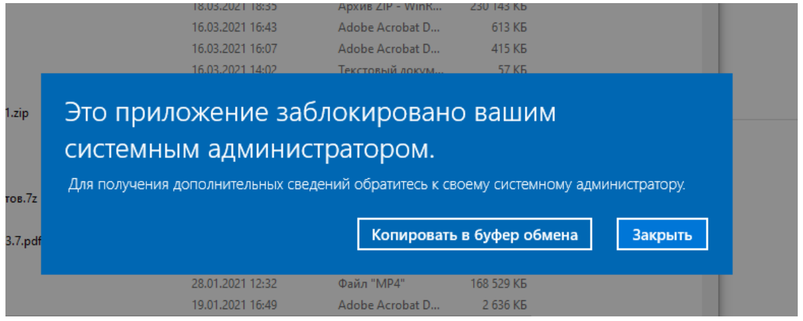
Windows

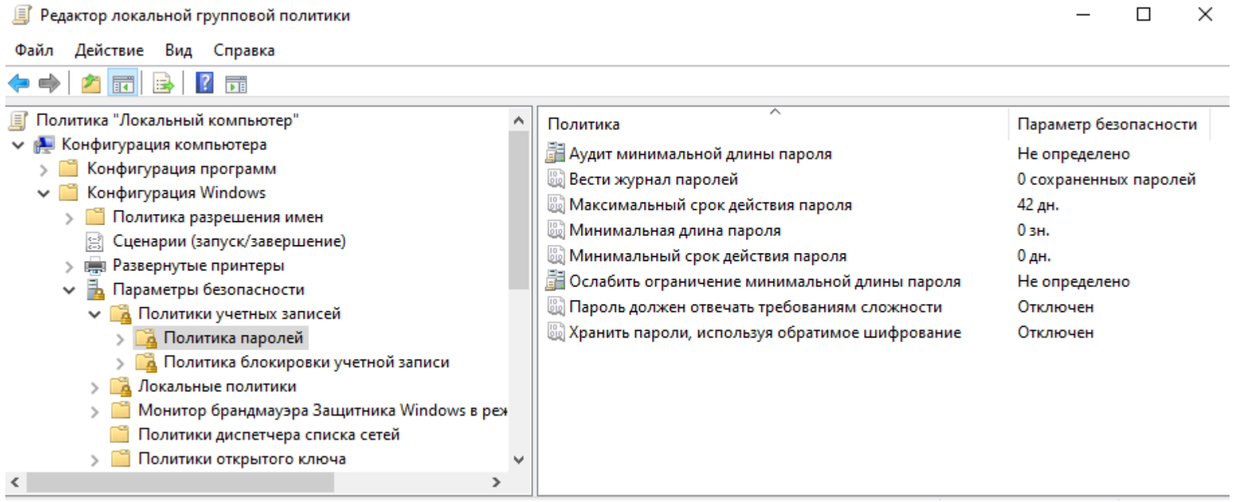
01 Белые списки

02 Парольная политика

03 Учётка админа







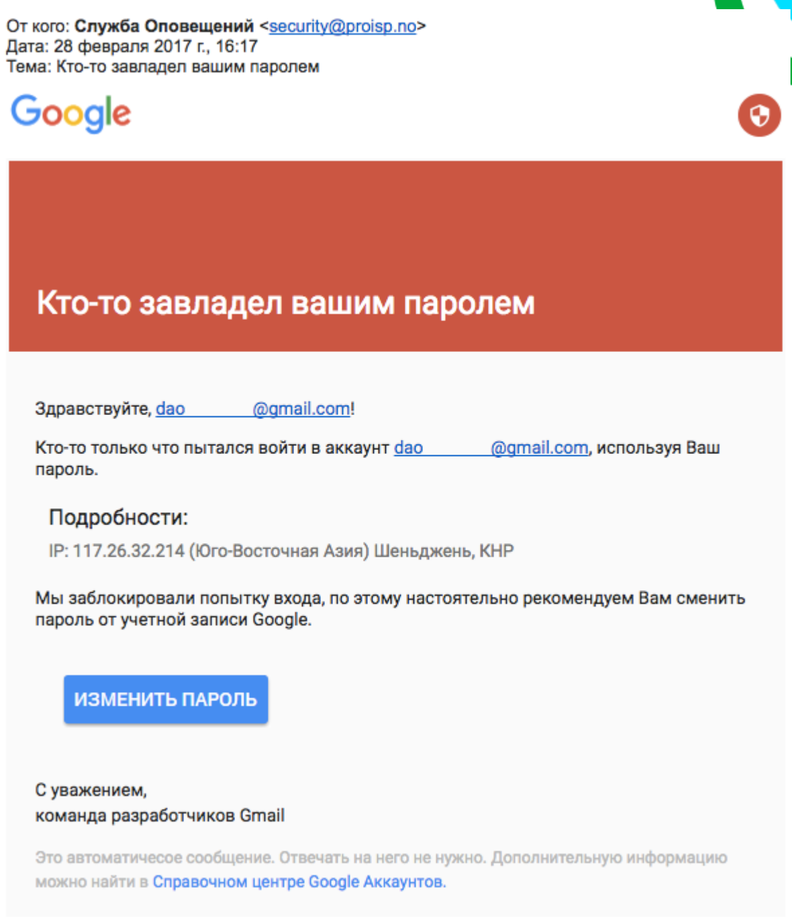
Окружение

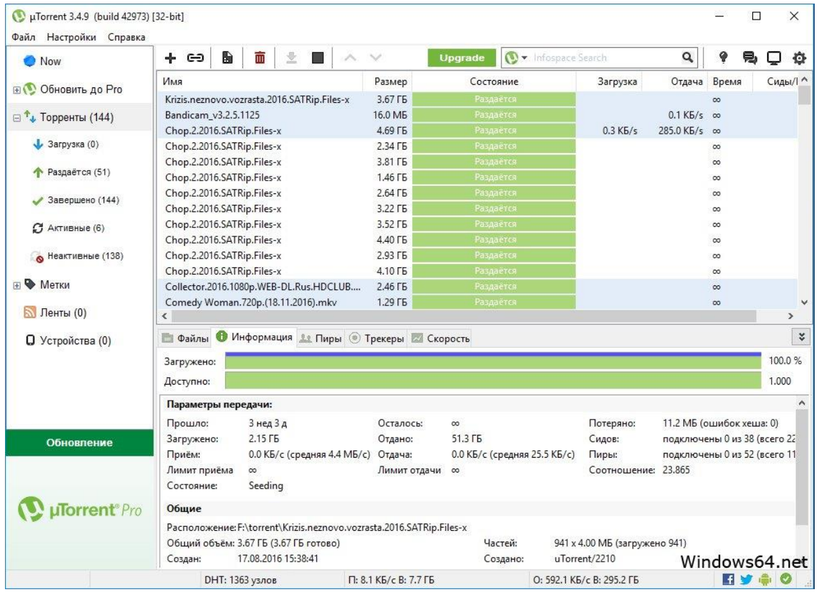
01 Proxy + репутация

02 Личная почта (фишинг)

03 Deep Packet Inspection

04 Домашний Wi-Fi роутер





Статистика

01 Риск поймать вредонос в домашней сети в 3,5 раза больше, чем в корпоративной

02 Более 25% устройств имеют открытые во вне сервисы, которые открытыми быть не должны

Some attributes of Work from Home - Remote Office Networks:

Malware:

- **3.5x more likely** than corporate networks to have at least one family of malware
- **7.5x more likely** to have at least five distinct families of malware
- Common families of malware are extremely prevalent including **Mirai**, which is observed **20x more frequently**, and **Trickbot** which is observed **3.75x more frequently**

Services & Remote Management Exposure:

- **More than 25%** of all devices have one or more services exposed on the internet
- **Almost 1 in 7** WFH-RO IP addresses have exposed cable modem control interfaces

https://www.bitsight.com/blog/identifying-unique-risks-of-work-from-home-remote-office-networks

После инцидента

Что используется на работе после заражения:

01 Endpoint Detection and Response (EDR)

02 SOC (Security Operations Center)

03 Блокировка сегментов на МЭ

Что делать?

01 Ввод личного ПК в домен организации

02 Выдача служебных ПК/ноутбуков

03 Работа через терминал

03 Типовое АРМ Чиновника (флешка + live_usb)

КОД безопасности

Спасибо за внимание!